

09/913695

Practitioner's Docket No. 13189.136

CHAPTER II

Preliminary Classification:

Proposed Class:

Unknown

Subclass:

Unknown

TRANSMITTAL LETTER
TO THE UNITED STATES ELECTED OFFICE (EO/US)
(ENTRY INTO U.S. NATIONAL PHASE UNDER CHAPTER II)

PCT/EP99/09977	15 December 1999 (15.12.99)	16 February 1999 (16.02.99)
International Application Number	International Filing Date	International Earliest Priority Date

TITLE OF INVENTION: METHOD AND DEVICE FOR GENERATING AN ENCRYPTED
USER DATA STREAM AND METHOD AND DEVICE FOR PLAYING
BACK AN ENCRYPTED USER DATA STREAM

APPLICANT(S): Rump, Niels; Koller, Juergen and Brandenburg, Karlheinz

ATTENTION: EO/US

Box PCT

Assistant Commissioner for Patents

Washington DC 20231

- I. Applicant herewith submits to the United States Elected Office (EO/US) the following items under 35 U.S.C. Section 371:
- This express request to immediately begin national examination procedures (35 U.S.C. Section 371(f)).
 - The U.S. National Fee (35 U.S.C. Section 371(c)(1)) and other fees (37 C.F.R. Section 1.492) as indicated below:

CERTIFICATION UNDER 37 C.F.R. SECTION 1.10*

(Express Mail label number is **mandatory**.)

(Express Mail certification is optional.)

I hereby certify that this paper, along with any document referred to, is being deposited with the United States Postal Service on this date Aug 16, 2001, in an envelope as "Express Mail Post Office to Addressee," mailing Label Number EL895408514US addressed to ATTENTION: EO/US, Box PCT, Assistant Commissioner for Patents, Washington, DC 20231.

Cheryl Martinez

(type or print name of person mailing paper)



Signature of person mailing paper

WARNING: Certificate of mailing (first class) or facsimile transmission procedures of 37 C.F.R. Section 1.8 cannot be used to obtain a date of mailing or transmission for this correspondence.

***WARNING:** Each paper or fee filed by "Express Mail" must have the number of the "Express Mail" mailing label placed thereon prior to mailing. 37 C.F.R. Section 1.10(b).

"Since the filing of correspondence under [Section] 1.10 without the Express Mail mailing label thereon is an oversight that can be avoided by the exercise of reasonable care, requests for waiver of this requirement will not be granted on petition." Notice of Oct. 24, 1996, 60 Fed. Reg. 56,439, at 56,442.

Doc. 1552

(Transmittal Letter to the United States Elected Office (EO/US)-page 1 of 3)

09/913695
531 Rec'd PCT 16 AUG 2001

2. Fees

CLAIMS FEE*	(1) FOR	(2) NUMBER FILED	(3) NUMBER EXTRA	(4) RATE	(5) CALCULATIONS
BASIC FEE	TOTAL CLAIMS	17 -20 =	0	x \$18.00 =	\$0.00
	INDEPENDENT CLAIMS	4 -3 =	1	x \$80.00 =	\$80.00
	MULTIPLE DEPENDENT CLAIM(S) (if applicable) + \$270.00				\$0.00
	U.S. PTO WAS NOT INTERNATIONAL PRELIMINARY EXAMINATION AUTHORITY Where no international preliminary examination fee as set forth in Section 1.482 has been paid to the U.S. PTO, and payment of an international search fee as set forth in Section 1.445(a)(2) to the U.S. PTO: where a search report on the international application has been prepared by the European Patent Office or the Japanese Patent Office (37 C.F.R. Section 1.492(a)(5)) \$860.00				\$860.00
SMALL ENTITY	Total of above Calculations				= \$940.00
	Reduction by 1/2 for filing by small entity, if applicable. Affidavit must be filed. (note 37 CFR Sections 1.9, 1.27, 1.28)				- \$0.00
	Subtotal				\$940.00
	Total National Fee				\$940.00
	Fee for recording the enclosed assignment document \$40.00 (37 C.F.R. Section 1.21(h)). See attached "ASSIGNMENT COVER SHEET".				\$0.00
TOTAL	Total Fees enclosed				\$940.00

*See attached Preliminary Amendment Reducing the Number of Claims.

Please charge Account No. 50-1848 in the amount of \$940.00.

A duplicate copy of this sheet is enclosed.

- A copy of the International Application as filed (35 U.S.C. Section 371(c)(2)) is transmitted herewith.
- A translation of the International Application into the English language (35 U.S.C. Section 371(c)(2)) is transmitted herewith.
- Amendments to the claims of the International application under PCT Article 19 (35 U.S.C. Section 371(c)(3)) have not been transmitted. Applicant chose not to make amendments under PCT Article 19.

Date of mailing of Search Report (from Form PCT/ISA/220): 7 September 2000.

- A translation of the amendments to the claims under PCT Article 19 (38 U.S.C. Section 371(c)(3)) has not been transmitted for reasons indicated in section 5.

09913695 080202
097 913695
531 Rec'd PCT 16 AUG 2001

7. A copy of the International Examination Report (PCT/IPEA/416) is transmitted herewith.
8. There were no Annexes to the International Preliminary Examination Report.
9. An oath or declaration of the inventor (35 U.S.C. Section 371(c)(4)) complying with 35 U.S.C. Section 115 will follow.
- II. Other document(s) or information included:
10. An International Search Report (PCT/ISA/220) or Declaration under PCT Article 17(2)(a) is transmitted herewith.
11. An Information Disclosure Statement under 37 C.F.R. Sections 1.97 and 1.98 will be transmitted within THREE MONTHS of the date of submission of requirements under 35 U.S.C. Section 371(c).
12. Additional documents:
 - a. International Publication No. WO 00/49762 (Front page only)
 - b. Preliminary amendment (37 C.F.R. Section 1.121)
 - c. Final version of PCT/EP99/09977 for the prosecution at the USPTO to be filed as first preliminary amendment
 - d. Annotated copy of Final version of PCT/EP99/09977
 - e. Express Mail Certificate
 - f. Return Postcard
13. The above items are being transmitted before 30 months from any claimed priority date.

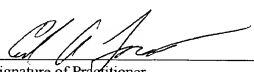
AUTHORIZATION TO CHARGE ADDITIONAL FEES

The Commissioner is hereby authorized to charge the following additional fees that may be required by this paper and during the entire pendency of this application to Account No. 50-1848:

- 37 C.F.R. Section 1.492(a)(1), (2), (3), and (4) (filing fees)
- 37 C.F.R. Section 1.492(b), (c), and (d) (presentation of extra claims)
- 37 C.F.R. Section 1.17 (application processing fees)
- 37 C.F.R. Section 1.17(a)(1)-(5) (extension fees pursuant to Section 1.136(a))
- 37 C.F.R. Section 1.492(e) and (f) (surcharge fees for filing the declaration and/or filing an English translation of an International Application later than 20 months after the priority date).

Date: Aug 16, 2001

Reg. No.: 28,494
Tel. No.: 303-379-1114
Fax No.: 303-379-1155



Signature of Practitioner
Carl A. Forest
Customer No.: 24283

09/913695

531 Rec'd PCT

16 AUG 2001

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
AS DESIGNATED/ELECTED OFFICE DO/EO/US

U.S. Patent Application No.: Applied For)	Group Art Unit: Unknown
International Application No.: PCT/EP99/0997)	Examiner: Unknown
International Filing Date: 15 December 1999)	Docket No: 13189.136
Priority Date: 16 February 1999)	
For: Method And Device For Generating An)	
Encrypted User Data Stream And Metho)	
And Device For Playing Back An)	
Encrypted User Data Stream)	
Applicants (Inventors):)	
Niels Rump, Juergen Koller and Karlhein)	
Brandenburg)	

ATTENTION: EO/US
BOX PCT
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, DC 20231

August 15, 2001

Dear Sir:

FIRST PRELIMINARY AMENDMENTIn the Specification:

Please substitute the attached specification entitled "Final version of PCT/EP99/09977 for the prosecution at the USPTO to be filed as first preliminary amendment" for the original PCT specification.

In the Claims:

Please substitute the enclosed claims 1 - 17, on pages 21 - 25, inclusive, attached to the substitute specification, for original claims 1 - 17.

U.S. Patent Application No.: Applied For
International Application No.: PCT/EP99/09977
First Preliminary Amendment

Page 1

Doc. 1555

In the Abstract:

Please substitute the enclosed abstract, attached to the substitute specification on page 26 for the original abstract.

REMARKS

Applicants respectfully request that the Examiner base the examination upon the attached substitute specification, claims, and abstract. An Annotated Copy Of Final Version Of PCT/EP99/09977 is enclosed showing the revisions made in the substitute specification, claims, and abstract.

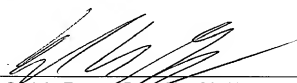
The PCT specification, claims, and abstract have been revised to conform to U.S. requirements. It is believed that no new matter was introduced in revising the specification, claims, and abstract.

In view of the foregoing amendments, it is believed that the application, including claims 1 – 17 is in condition for allowance, and favorable action is respectfully requested. The Examiner is invited to contact the undersigned by collect telephone call to advance the prosecution in any respect.

No additional fee for this Preliminary Amendment is seen to be required. If any additional fee is required, please charge it to Deposit Account No. 50-1848.

Respectfully submitted,
PATTON BOGGS LLP

By: _____


Carl A. Forest, Reg. No. 28,494
Telephone: (303) 379-1114
Facsimile: (303) 379-1155
Customer No.: 24283

U.S. Patent Application No.: Applied For
International Application No.: PCT/EP99/09977
First Preliminary Amendment

Page 2
Doc. 1555

Such applications have been filed as follows.

**PRIOR PCT APPLICATION(S) FILED WITHIN 12 MONTHS
(6 MONTHS FOR DESIGN) PRIOR TO THIS APPLICATION
AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. SECTION 119(a)-(d)**

INDICATE IF PCT	APPLICATION NUMBER	DATE OF FILING DAY, MONTH, YEAR	PRIORITY CLAIMED UNDER 35 U.S.C. SECTION 119
PCT	PCT/EP99/09977	15 December 1999	yes

**PRIOR FOREIGN APPLICATION(S) FILED WITHIN 12 MONTHS
(6 MONTHS FOR DESIGN) PRIOR TO THIS APPLICATION
AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. SECTION 119(a)-(d)**

COUNTRY	APPLICATION NUMBER	DATE OF FILING DAY, MONTH, YEAR	PRIORITY CLAIMED UNDER 35 U.S.C. SECTION 119
Germany	19906449.0	16 February 1999	yes

POWER OF ATTORNEY

I hereby appoint the practitioner(s) associated with the Customer Number provided below to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

Customer No. 24283

SEND CORRESPONDENCE TO:
Customer No. 24283

DIRECT TELEPHONE CALLS TO:
Carl A. Forest
303-379-1114

DECLARATION

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

SIGNATURE(S)

1-00
Niels Rump

Inventor's signature Niels Rump

Date 2002-03-19

Residence Kent United Kingdom GBx Country of Citizenship Germany

Post Office Address 16 Chatsworth Avenue, Bromley, Kent BR1 1DP United Kingdom

COMBINED DECLARATION AND POWER OF ATTORNEY**(ORIGINAL, DESIGN, NATIONAL STAGE OF PCT, SUPPLEMENTAL, DIVISIONAL,
CONTINUATION, OR C-I-P)**

As a below named inventor, I hereby declare that:

TYPE OF DECLARATION

This declaration is for a national stage of PCT application.

INVENTORSHIP IDENTIFICATION

My residence, post office address and citizenship are as stated below, next to my name. I believe that I am an original, first and joint inventor of the subject matter that is claimed, and for which a patent is sought on the invention entitled:

TITLE OF INVENTION

METHOD AND DEVICE FOR GENERATING AN ENCRYPTED USER DATA STREAM AND
METHOD AND DEVICE FOR PLAYING BACK AN ENCRYPTED USER DATA STREAM

SPECIFICATION IDENTIFICATION

The specification was filed on August 16, 2001, as Serial No. 09/913,695

ACKNOWLEDGMENT OF REVIEW OF PAPERS AND DUTY OF CANDOR

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information, which is material to patentability as defined in 37, Code of Federal Regulations, Section 1.56, and which is material to the examination of this application, namely, information where there is a substantial likelihood that a reasonable Examiner would consider it important in deciding whether to allow the application to issue as a patent.

PRIORITY CLAIM (35 U.S.C. Section 119(a)-(d))

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d) of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed.

Such applications have been filed as follows.

**PRIOR PCT APPLICATION(S) FILED WITHIN 12 MONTHS
(6 MONTHS FOR DESIGN) PRIOR TO THIS APPLICATION
AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. SECTION 119(a)-(d)**

INDICATE IF PCT	APPLICATION NUMBER	DATE OF FILING DAY, MONTH, YEAR	PRIORITY CLAIMED UNDER 35 U.S.C. SECTION 119
PCT	PCT/EP99/09977	15 December 1999	yes

**PRIOR FOREIGN APPLICATION(S) FILED WITHIN 12 MONTHS
(6 MONTHS FOR DESIGN) PRIOR TO THIS APPLICATION
AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. SECTION 119(a)-(d)**

COUNTRY	APPLICATION NUMBER	DATE OF FILING DAY, MONTH, YEAR	PRIORITY CLAIMED UNDER 35 U.S.C. SECTION 119
Germany	19906449.0	16 February 1999	yes

POWER OF ATTORNEY

I hereby appoint the practitioner(s) associated with the Customer Number provided below to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

Customer No. 24283

SEND CORRESPONDENCE TO:
Customer No. 24283

DIRECT TELEPHONE CALLS TO:
Carl A. Forest
303-379-1114

DECLARATION

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

SIGNATURE(S)

Niels Rump

Inventor's signature _____

Date _____

Country of Citizenship Germany

Residence Erlangen Germany

Post Office Address Brueckenstrasse 13, Erlagen D-91056 Germany

2-00
Juergen Koller

Inventor's signature _____

Date September 24, 2001

Country of Citizenship Germany

Residence Erlangen Germany

Post Office Address St. Johann 6/113, Erlangen D-91054 Germany

3-00
Karlheinz Brandenburg

Inventor's signature _____

Date September 24, 2001

Country of Citizenship Germany

Residence Erlangen Germany

Post Office Address Haagstrasse 32, Erlangen D-91054 Germany

**SIGNATURE BY JOINT INVENTOR(S) ON BEHALF OF NONSIGNING
INVENTOR(S) WHO CANNOT BE REACHED
(37 C.F.R. section 1.47(a))**

- I. I am an above named joint inventor and have signed this declaration on my own behalf and also sign this declaration under 37 C.F.R. section 1.47(a) on behalf of the nonsigning joint inventor, particulars for whom are:

Niels Rump, nonsigning inventor who cannot be found or reached.

Country of Citizenship of nonsigning inventor:

Germany

Last known address of nonsigning inventor:

Brueckenstrasse 13

Erlagen, D-91056 Germany

- II. Accompanying this declaration is:

- (1) A STATEMENT OF FACTS IN SUPPORT OF FILING ON BEHALF OF NONSIGNING INVENTOR.
- (2) THE PETITION FEE OF \$130.00 (37 C.F.R. Section 1.17(i)).

Date: September 24, 2001

Signature


Juergen Koller

Date: September 24, 2001

Signature


Karlheinz Brandenburg

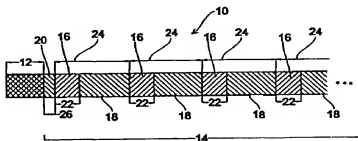


PCT
WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro
INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE
INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

<p>(51) Internationale Patentklassifikation 7 : H04N 7/16, H04H 1/00</p>	A3	<p>(11) Internationale Veröffentlichungsnummer: WO 00/49762</p> <p>(43) Internationales Veröffentlichungsdatum: 24. August 2000 (24.08.00)</p>
<p>(21) Internationales Aktenzeichen: PCT/EP99/09977</p> <p>(22) Internationales Anmeldedatum: 15. Dezember 1999 (15.12.99)</p> <p>(30) Prioritätsdaten: 199 06 449.0 16. Februar 1999 (16.02.99) DE</p> <p>(71) Anmelder (für alle Bestimmungsstaaten ausser US): FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V. [DE/DE]; Leonrodstrasse 54, D-80636 München (DE).</p> <p>(72) Erfinder; und (75) Erfinder/Anmelder (nur für US): RUMP, Niels [DE/DE]; Brückenstrasse 13, D-91056 Erlangen (DE). KOLLER, Jürgen [DE/DE]; St. Johann 6/113, D-91054 Erlangen (DE). BRANDENBURG, Karlheinz [DE/DE]; Haagstrasse 32, D-91054 Erlangen (DE).</p> <p>(74) Anwalt: SCHOPPE, Fritz; Schoppe, Zimmermann & Stöckeler, Postfach 71 08 67, D-81458 München (DE).</p>	<p>(81) Bestimmungsstaaten: JP, KR, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).</p> <p>Veröffentlicht <i>Mit internationalem Recherchenbericht.</i></p> <p>(88) Veröffentlichungsdatum des internationalen Recherchenberichts: 9. November 2000 (09.11.00)</p>	

(54) Title: **METHOD AND DEVICE FOR GENERATING AN ENCODED USEFUL DATA STREAM AND METHOD AND DEVICE FOR PLAYING BACK AN ENCODED USER DATA STREAM**

(54) Bezeichnung: **VERFAHREN UND VORRICHTUNG ZUM ERZEUGEN EINES VERSCHLÜSSELTEN NUTZDATENSTROMS UND VERFAHREN UND VORRICHTUNG ZUM ABSPIELEN EINES VERSCHLÜSSELTEN NUTZDATENSTROMS**



(57) Abstract

The invention relates to a method for generating an encoded multimedia data stream, according to which first a start block (12) and then a user data block (14) are generated. The initial segment (20) of the user data block (20) contains unencoded user data which are followed by encoded user data (16). In this way a preview or prelist function can be implemented in a simple manner. In addition, a playback device can already play back the unencoded initial section (20) while the complete start block is being processed so as to obtain a multimedia data key for generating hash totals, etc. The above parallel processing makes it possible to use playback devices with limited storage and processing resources without having to accept excessively long delays.

09913695.080202

09/913695

531 Rec'd PCT. 16 AUG 2001

National Phase of PCT/EP99/09977 in U.S.A.

Title: Method and Device for Generating an Encrypted User
Data Stream and Method and Device for Playing Back an
Encrypted User Data Stream

Applicants: RUMP, Niels et al.

Final version of PCT/EP99/09977 for the prosecution at the
USPTO to be filed as first preliminary amendment

09/913695
531 Rec'd PCT/PTC 16 AUG 2001

**Method and Device for Generating an Encrypted User Data Stream
and Method and Device for Playing Back an Encrypted User Data
Stream**

Description

The present invention relates to the encrypting and decrypting of user data and in particular to the handling of encrypted user data streams with a start block and a user data block.

With the appearance of telecommunication networks and in particular because of the widespread use of personal computers capable of handling multimedia data and, more recently, also of so-called solid state players, a need has arisen to commercially exploit digital multimedia data, such as digital audio data and/or digital video data. The telecommunication networks might be e.g. analog telephone lines, digital telephone lines, such as ISDN, or the internet. Among commercial suppliers of multimedia products there is the need to sell or hire out multimedia data within a framework where a customer can select a particular product from a particular catalogue at any time, which product can then, of course, only be used by the customer who has paid for it.

In contrast to known encrypted television programs, such as those from the television channel Premiere, where the transmitted data are encrypted identically for all the users who have acquired a suitable decrypting device by paying a certain charge, the objective of the present invention is to provide methods and devices which offer an individual, customer-specific and secure encrypting and decrypting of multimedia data. In contrast to the cited television channels, which provide a fixed program which the customer must accept as a package, the methods and devices of the present invention allow

the customer maximum flexibility, i.e. he only has to pay for those products which he actually wishes to use.

DE 196 25 635 C1 describes methods and devices for encrypting and decrypting multimedia data where the multimedia data are in the form of an encrypted multimedia file with a definition data block and a user data block. Parts of the definition data block and parts at least of the user data block are encrypted with different keys and symmetric encrypting methods are chiefly used.

An advantage of symmetric encrypting methods is that they are relatively quick. On the other hand the user who wishes to decrypt the file needs the same key as the provider or supplier, e.g. Deutsche Telekom, who has encrypted the multimedia data, in order to sell them to the customer. Thus both the provider and the user, i.e. the customer, have one table with a plurality of possible symmetric encryption algorithms, such as DES or Blowfish, and another table for possible keys. The provider generates an entry in the definition data block of the multimedia data which the user then uses to access his key table so as to select the correct key for decrypting.

In response to the rapidly increasing deployment of the MP3 standard, so-called solid state players for decrypting and playing back multimedia data have appeared on the market. These players are meant to be very inexpensive, so they are restricted as to memory and computing power. In contrast to personal computers, which have resources far in excess of those needed for the decrypting of multimedia data, solid state players or stereo systems or car hifi units must be cheap to buy if they are to be successful in a very competitive market. These devices must therefore be designed to decrypt multimedia data and play back the decrypted data using the minimum possible computing power and memory.

A disadvantage of the encrypting and decrypting concept in DE 196 25 635 C1 is the fact that the whole of the definition data block has to be processed before it is possible to start decrypting the user data block, decoding the decrypted user data block and, finally, playing back the decrypted decoded user data block.

This becomes a particular problem if the processing of the definition data block in a decrypting device entails substantial computing operations, e.g. calculating a hash total or a fingerprint of the start block. The situation could become even more serious if the decrypting device has only limited storage and processing resources. However, limited storage and processing resources are just what playback devices, in particular solid state players, should have if they are to be marketable in an inexpensive form.

A further disadvantage of the known encrypting and decrypting concept is the fact that a simple preview or prelisten function poses a problem. If the multimedia data are video data, it is sometimes desirable to be able to look at the first, say, 10 or 20 seconds, either to provide a basis for deciding whether to purchase the piece being offered or so as to make it possible to identify a particular piece. If the multimedia data are audio data, there is a need to be able to "listen into" a piece, i.e. to listen to the first, say, 10 or 20 seconds before deciding whether the piece should be purchased or so as to identify the piece.

It is the object of the present invention to provide a concept for generating and playing back encrypted multimedia data streams which manages to do so with moderate storage and processing resources and which also permits an efficient implementation of a preview or prelisten function.

This object is achieved by a method for generating an encrypted user data stream according to claim 1, by a method for playing back an encrypted user data stream according to claim 6, by a device for generating an encrypted user data stream according to claim 12 and by a device for playing back an encrypted user data stream according to claim 13.

The present invention is based on the finding that the concept that the user data are encrypted right from the start must be abandoned. In the prior art the aspiration was always to encrypt the user data right from the start in order to protect the whole user data block, and especially the initial part of it, from unauthorized access.

It should be noted that while user data generally refers to multimedia data, i.e. audio data, video data or a combination of audio and video data, it also includes e.g. text data. On the grounds of expediency, however, the subject matter of the present invention will be explained in terms of multimedia data. It is, however, apparent that all types of user data for which there is a need for encryption can be processed by the devices and methods of the present invention.

It was discovered, however, that the delay arising from the processing of the start block can become significant, especially when this involves complex operations such as forming hash totals, the more so when playback devices with limited storage and processing resources are to be used.

It was also discovered that the demands made on the processing capacity of a processor with limited processing power are particularly high when processing the start block but are lower when decrypting, decoding and playing back the decrypted decoded multimedia data. This means that a relatively high proc-

essing power must be provided only for the processing of the start block and that this is no longer fully exploited when decrypting, decoding and playing back the data stream. It should be noted that the security of an encrypted multimedia data stream is essentially ensured by the start block, i.e. that it is always advisable to employ a relatively high computing power to process this block in order to achieve secure concepts. For this reason it is not desirable that the processing of the start block in general should be simplified so as to reduce the delay arising from the processing of the start block.

According to the present invention a certain section which commences at the beginning of the multimedia data to be encrypted, i.e. at the beginning of a user data block, and which terminates after a predetermined duration of the multimedia data to be encrypted, i.e. a first part of the multimedia data to be encrypted, is not therefore encrypted but is written unencrypted into a start section of the user data block of the encrypted multimedia data. Encryption commences only with the multimedia data which follow the first part, these being encrypted in a suitable manner and appended to the start section of the user data block. This means that the first part of a multimedia data item, normally within the range from 5 to 20 seconds, is freely accessible. The demands made on the processor in order to play back this first part are minimal since no hash totals have to be calculated and no encrypted multimedia key has to be decrypted, etc. Furthermore, at this stage it is not absolutely necessary to process elaborate licence data relating to the authorized use of the multimedia data stream. A playback device will therefore be able to play back the first part of the multimedia data without any significant delay. Accordingly, it is already possible to achieve an effective preview or prelisten function in a simple and efficient manner.

Providing an unencrypted start section of the user data block brings further significant advantages, however, if the decrypting devices have only limited storage and processing resources, which is very much the case for solid state players, which must be put on the market at the lowest possible price. If multimedia data to be encrypted are coded with some sort of MPEG method, for example, a playback device simply has to decode and play back the multimedia data in order to be able to play back the start section of the user data block. The playback device thus has processing resources available during the decoding and playback phase with which it can fully process the start block itself while the start section of the user data block, which is unencrypted, is being played back. It can then decrypt, decode and play back the subsequent encrypted part of the user data block.

The provision according to the present invention of an unencrypted start section of the user data block therefore makes it possible to allocate the necessary storage and processing resources in such a way that, even with playback devices with limited resources, it is possible to decrypt, decode and play back multimedia data without excessively long delay.

Preferred embodiments of the present invention are described in detail below making reference to the enclosed drawings, in which

Fig. 1 shows a multimedia data stream, which can be generated according to the present invention;

Fig. 2 shows a detailed representation of the start block and of the user data block of the encrypted multimedia data stream;

Fig. 3 shows a selection of some of the entries in the individual subblocks of the start block;

Fig. 4 shows a flowchart of the method of generating an encrypted multimedia data stream according to the present invention; and

Fig. 5 shows a flowchart of the method of playing back an encrypted multimedia data stream according to the present invention.

Fig. 1 shows an encrypted multimedia data stream 10, which has a start block or header 12 and a user data block 14, i.e. a block with encrypted multimedia data. The user data block 14 encompasses encrypted sections 16 and unencrypted sections 18 between the encrypted sections 16. Furthermore, a multimedia data stream which can be generated according to the present invention also has a further unencrypted section 20, which follows the start block 12 and precedes an encrypted section 16.

Normally the multimedia data to be encrypted are coded in some way, e.g. according to an MPEG standard such as MPEG-2 AAC, MPEG-4 AAC or MPEG layer 3. It suffices therefore to encrypt just certain sections of the multimedia data to be encrypted. This leads to a considerably reduced processing effort both on the part of the provider, who encrypts the data, and on the part of the customer, who must decrypt the data again. Apart from this, as a consequence of the only partial encryption of the multimedia data the pleasure which a user who utilizes only the unencrypted multimedia data enjoys, whether listening or viewing, is severely impaired due to the encrypted blocks, which appear at regular intervals.

Although Fig. 1 shows an encrypted multimedia data stream wherein the start block 12 is at the start of the encrypted multimedia data stream, this arrangement of start block and user data block should not be taken to relate to the transmission of the encrypted multimedia data stream. The expression "start block" is merely meant to indicate that a decrypting device which wishes to decrypt the encrypted multimedia data stream first requires at least parts of the start block before the multimedia data themselves can be decrypted. Depending on the transmission medium, the start block could also be located somewhere within the user data block or could well be received after certain parts of the user data block, e.g. in the case of a packet-oriented transmission of the multimedia data stream where different packets, one of which may contain the start block and some other may contain part of the user data block, are transmitted over different physical transmission paths and where there is absolutely no need for the received sequence to correspond to the transmitted sequence. In this case a decrypting device must, however, be capable of storing the received packets and rearranging them in such a way that information can be extracted from the start block so as to be able to start decrypting. The encrypted multimedia data stream might also take the form of a file or it might also take the form of an actual data stream, e.g. in the case of a live transmission of a multimedia event. This application will feature particularly in the case of digital user-selective broadcasting.

The length of an encrypted section 16 is represented by a value Amount 22, while the interval in the encrypted multimedia data stream from the start of an encrypted section 16 to the start of the next encrypted section 16 is indicated by Step 24. The length of the further unencrypted section 20 is given by a value First step 26.

These values 22, 24 and 26 are, of course, needed for the correct decryption of the multimedia data in a decrypting device, which is why these values must be entered in the start block 12, as will be explained later.

It should be noted, however, that the relative sizes of the values 22 and 24 can be variable. One of the possibilities is that the length of the unencrypted section 18 is zero, i.e. that encryption is complete.

Fig. 2 shows a more detailed representation of the encrypted multimedia data stream 10, which comprises the start block 12 and the user data block 14. The start block 12 is subdivided into a number of subblocks, which will be described individually with especial reference to Fig. 3. Attention is drawn to the fact that the number and function of the subblocks can be expanded without restriction. Just some of these subblocks of the start block 12 are therefore shown as an example in Fig. 2. As shown in Fig. 2 the start block 12 includes a so-called crypt block 28, which, roughly speaking, contains information which is relevant to the encryption of the multimedia data. The start block 12 also has a so-called licence block 30, which contains data relating to the way in which a user can or may utilize the encrypted multimedia data stream. The start block 12 also includes a user data info block 32, which can include information relating to the user data block 14 and general information on the start block 12 itself. In addition, the start block 12 may also have an old-start-block block 34, which permits a so-called recursive start block structure. This block enables the user who has not only a decrypting device but also an encrypting device to reformat an encrypted multimedia data stream for other playback devices in his possession without losing or modifying the start block information originally supplied by the distributor. Depending on the application, further subblocks, e.g. an IP information block

(IP = Intellectual Property) according to ISO/IEC 14496-1, MPEG-4, Systems, 1998, which contains copyright information, can be included in the start block 12.

As is customary in the field of technology, each block can be designed to have an internal block structure, which first requires a block identifier, then contains the length of the subblock, and then, finally, presents the block user data as such. This increases the flexibility of the encrypted multimedia data stream and in particular that of the start block of the encrypted multimedia data stream in that new demands can be responded to by adding further subblocks and omitting existing subblocks.

Fig. 3 provides an overview of the block user data of the individual subblocks shown in Fig. 2.

The crypt block 28 is considered first. This contains an entry for a multimedia data encryption algorithm 40 which identifies the symmetric encryption algorithm which has been used to encrypt the multimedia data in a preferred embodiment of the present invention. The entry 40 may well be an index for a table such that a decrypting device having read the entry 40 is able to select from among a plurality of encryption algorithms the same encryption algorithm at that used by the encrypting device. The crypt block 28 also includes the entry First step 26, the entry Step 24 and the entry Amount 22, which have already been referred to in connection with Fig. 1. These entries in the start block enable a decrypting device to subdivide an encrypted multimedia data stream appropriately so as to be able to perform decryption correctly.

The crypt block 28 also contains an entry for the distributor or provider or supplier 42 which is a code for the distributor who has generated the encrypted multimedia data stream. An en-

try User 44 identifies the user who has received the encrypted multimedia data stream in some way or other from the distributor identified by the entry 42. One possible use for these identifiers is to make the user identification device-specific. The entry User would then contain the serial number of a PC, a laptop, a car hifi device, a home stereo system, etc., which only permits playback on the specific device. To further improve the flexibility and/or security, instead of using the serial number, which has a different structure from one manufacturer to another, but which could be duplicated by chance, a special identification, e.g. a logical coupling of the size of the fixed disk with the processor number etc. in the case of a PC, could be used instead.

An entry 46 contains an output value, which will be discussed in more detail later. This output value represents, generally speaking, an encrypted version of the multimedia data key, which is needed, in conjunction with the multimedia data encryption algorithm identified by the entry 40, in order to correctly decrypt the encrypted multimedia data (sections 16 in Fig. 1) in the user data block 14. To ensure adequate flexibility for future applications, the two entries Output value length 48 and Output value mask 50 have been provided. The entry Output value length 48 indicates the actual length of the output value 46. However, to achieve a flexible start block format more bytes are provided therein for the output value than an output value can actually have at the present time. The output value mask 50 thus indicates how a shorter output value is distributed over a longer output value space. If the output value length is e.g. half as big as the space available for the output value, the output value mask could be so constituted that the first half of the output value mask is set and the second half is not set. The output value would then simply be entered in the space allocated by the syntax for the start block and occupy the first half of this space

while the other half is ignored due to the output value mask 50.

The licence block 30 of the start block 12 will now be considered. This includes an entry Bit mask 52. This entry can contain certain special information for playing back or for the general mode of using the encrypted multimedia data. In particular, a decrypting device could be informed in this way whether or not the user data can be played back locally. Furthermore, it could be signalized here whether the challenge-response method described in the German Patent DE 196 25 635 C1 cited earlier and which permits efficient database access has been used for encryption.

An entry Expiration date 54 indicates the date on which permission to decrypt the encrypted multimedia data stream expires. A decrypting device will check the entry Expiration date 54 and compare it with a built-in timer. If the expiration date has been passed, the decrypting device will no longer perform a decryption of the encrypted multimedia data stream. This enables a provider to supply encrypted multimedia data for a limited time period, offering the advantage of a much greater flexibility in the management of the data and in pricing policy. This flexibility is further supported by an entry Start date 56, which specifies when decryption of a encrypted multimedia file may commence. A decrypting device will compare the entry Start date with its own built-in clock and will only start decrypting the encrypted multimedia data when the actual time is later than that specified by the start date 56.

An entry Permitted playbacks 58 specifies how often the encrypted multimedia data stream may be decrypted, i.e. played back. This further increases the flexibility of the provider in that he only permits a certain number of playbacks, e.g. in

return for a certain sum which is less than that which would be demanded for the unrestricted use of the encrypted multimedia data stream.

To verify or support the entry Permitted playbacks 58 the licence block 30 has another entry Actual playbacks 60, which could e.g. be incremented by one after each decryption of the encrypted multimedia data stream. A decrypting device will thus always check whether the entry Actual playbacks is less than the entry Permitted playbacks. If this is so, the multimedia data will be decrypted. If not, no further decryption takes place.

The entries Permitted copies 62 and Actual copies 64 are analogues of the entries 58 and 60. By means of the two entries 62 and 64 it is ensured that the user of the multimedia data only copies them as often as he is allowed to do so by the provider or as often as is warranted by the cost of buying the multimedia data. By means of the entries 58 to 64 an effective copyright protection is guaranteed and it is possible to discriminate between private users and commercial users, e.g. by setting the entries Permitted playbacks 58 and Permitted copies 62 to a small value.

Licensing might e.g. be on the basis that a certain number of copies (entry 62) of the original is permitted while no copies of a copy are allowed. The start block of a copy would then, in contrast to the start block of the original, have a zero in the entry Permitted copies, meaning that this copy will not be copied again by a correctly functioning encrypting/decrypting device.

In the example of a multimedia data protection protocol (MMP; MMP = Multimedia Protection Protocol) shown here, the start block 12 also contains a user data information block 32 which

has just two block user data entries 66 and 68, the entry 66 containing a hash total over the whole start block and the entry 68 identifying the type of hash algorithm which has been used to generate the hash total over the whole start block.

Among the publications which are useful in this connection is the technical book "Applied Cryptography", Second Edition, John Wiley & Sons, Inc. By Bruce Schneier (ISBN 0 471-11709-9) which contains a comprehensive treatment of symmetric encryption algorithms, asymmetric encryption algorithms and hash algorithms.

Finally the start block 12 includes the old-start-block block 34, which in addition to the synchronization information, which is not shown in Fig. 3, contains the entry Old start block 70. If a user performs his own encryption and thus generates a new start block 12, the old start block from the provider can be preserved in the entry Old start block 70 so as not to lose any important information that the provider has written into the start block. This might include copyright information (IP information block), previous user information and distributor information, which make it possible to trace back a multimedia file, which e.g. has been de-crypted/encrypted several times by various devices, to the original supplier while preserving copyright information. In this way it is possible to check at all times whether an encrypted multimedia file has been acquired legally or illegally.

It is obvious that the sequence of steps in Fig. 5 can be varied in the same way as explained below with reference to Fig. 4.

Fig. 4 shows a flowchart of the method according to the present invention for generating an encrypted multimedia data

stream. In a step 100 the start block 12 is generated. Then, in a step 102, the first part of the multimedia data to be encrypted is used as the start section of the user data block 14, but this first part itself is not encrypted. The start section thus forms the further unencrypted section 20 of Fig. 1, whose length is specified in the entry First step 26 in the start block. The second part of the multimedia data to be encrypted is then encrypted in a step 104 to generate the encrypted section 16 which follows the unencrypted section 20 (Fig. 1). To produce a simple encrypted multimedia data stream, the encrypted second part is appended to the start section of the user data block (step 106), so that the encrypted multimedia data stream 10 contains the start block 12, the start section 20 and the encrypted second part 16. The encrypted multimedia data stream can now be extended as desired by generating another unencrypted section 18, an encrypted section 16, etc. and writing them into the user data block 14.

From Fig. 4 it can be seen that there is no fixed sequence for the steps 100 to 106. The start block could also be generated after completion of the user data block and placed at the head of the user data block using a block multiplexer. Alternatively, the second part of the multimedia data to be encrypted could be encrypted (step 104) before the first part is written into the data block since the entry First step 26 defines precisely the point, i.e. the bit position, in the data block 14 at which the encrypted second part must start to be entered. What is important here is simply that the unencrypted start section 20 of the user data block 14 should be placed immediately after the start block 12. It should be emphasized again at this point that the sequence of start block, unencrypted start section and encrypted second part (i.e. 12, 20, 16) described here simply describes the sequence in which the multimedia data stream must be arranged in the playback device so as to exploit the advantages of the present invention. This

sequence has no effect on the transmission of the encrypted multimedia data stream. This becomes particularly apparent when a packet-oriented transmission is used. A packet for the start block, a packet for the start section and a packet for the encrypted second part could be transmitted over different paths from a transmitter to a receiver in such a way that the start section arrives first, followed by the encrypted second part and finally the start block. In this case, of course, the playback device must be capable of rearranging the three packets, as has already been described.

Fig. 5 shows a flowchart of the method according to the present invention for playing back the encrypted multimedia data stream 10 comprising the start block 12, the unencrypted start section 20 of the user data block 14 and the encrypted second part 16 of the user data block 14. According to the present invention only the information of the start block 12 which is absolutely necessary for playing back the unencrypted start section of the user data block 14 (step 110) is initially processed in the playback device.

Subsequently the unencrypted start section 20 of the user data block 14 can be played back with minimal delay (step 112). In this way a simple and efficient preview or prelisten function is achieved. Playing back the start section of the user data block (step 112) will not normally require the full processing power of the playback device. Thus the playback device can, while playing back the start section, also process essentially concurrently the other information of the start block 12, i.e. the information which is not needed to play back the start section of the user data block (step 114). Once the start block 12 has been processed, the playback device will then be able to decrypt the encrypted multimedia data in the first encrypted section 16, i.e. the encrypted second part of the user data block 14 (step 116), thus enabling it to then play back

the decrypted multimedia data of the second section (step 118).

The information which is absolutely necessary for playing back the unencrypted start section 20 will now be discussed making reference to Fig. 3. Among the information which is absolutely necessary are the general block identification information and block length information, which are not shown in Fig. 3, which enable a playback device to correctly locate where the necessary information is to be found in the start block. If the multimedia data are coded in some way, as is usually the case, e.g. according to an MPEG method, the playback device will have to extract this information from the start block 12 in step 110 (Fig. 5). In the table in Fig. 3 this information is contained in the entry User data type of the user data block 14. The playback device then knows that the unencrypted data in the start section 20 of the user data block 14 are coded in e.g. MPEG layer 3 format (MP3), so that the playback device can then decode and play back the unencrypted multimedia data (step 112). While the start section 20 is being played back the device is now able to process all the relatively complicated additional data of the start section, such as the data in the crypt block 28, in the licence block 30 and in the user data information block 32, which in particular contains a relatively complex hash total /digital signature over the start block (entry 66). Another complicated operation is that of decrypting the multimedia data key from the output value (entry 46) so as to be able to decrypt the encrypted sections 16 (Fig. 1) of the encrypted multimedia data stream.

It is possible to specify whether or not the entries Distributor 42 and User 44 should also belong to the necessary information for playing back the unencrypted start section 20. If so, the preview or prelisten function is only available for a particular user or for the subscribers of a particular dis-

tributor. This means that, via the very simple and uncomplicated implementation of the preview or prelisten function, a distributor can send an encrypted multimedia file to a special user or to all his subscription users, who can then listen to or view an extract of e.g. 1 second's to 1 minute's duration, i.e. the unencrypted start section 20. If a user finds this offering to his taste he can then decide to pay for the whole encrypted multimedia data stream. This facility also enables individual items to be identified in a simple manner.

In this case it is not necessary to perform the steps 114, 116 and 118. It should be noted that it is in fact not possible to perform these steps in this case, since the user may not yet possess the information as to how the output value 46 must be decrypted so as to obtain the multimedia data key enabling the encrypted multimedia data in the encrypted sections 16 to be decrypted. Should a user decide to purchase after his appetite has been whetted by the preview or prelisten function, all the distributor has to do is to enable the user to decrypt the output value.

Providing an unencrypted start section in the user data block thus enables the preview or prelisten function to be offered in a simple way and also makes it possible to use processors with limited storage or processing resources without having to put up with significant delays resulting from the processing of the whole start block.

Claims

1. A method for generating an encrypted user data stream (10), which has a start block (12) and a user data block (14), comprising the following steps:

generating (100) the start block (12); and

generating (102, 104, 106) the user data block (14) by means of the following substeps:

using (102) a first part of the user data to be encrypted as start section (20) for the user data block (14), the start section (20) being unencrypted;

encrypting (104) a second part of user data to be encrypted which follow the first part; and

appending (106) the encrypted user data (16) to the unencrypted start section (20).

2. A method according to claim 1, wherein the step of generating (100) the start block (12) includes the following substep:

entering the length (26) of the start section (20) in the start block (12).

3. A method according to claim 1 or 2, wherein the second part does not comprise all the user data to be encrypted and wherein the step of generating (102, 104, 106) the user data block includes the following substep:

appending a third part (18) of user data to be encrypted,

which follow the second part, to the encrypted user data (16) of the second part, the user data of the third part being unencrypted.

4. A method according to one of the preceding claims, wherein the step of generating (100) the start block (12) includes the following substep:

entering the length (22) of the encrypted multimedia data (16), which correspond to the user data of the second part which are to be encrypted, in the start block (12).

5. A method according to claim 3 or 4, wherein the step of generating (100) the start block (12) also includes the following substep:

entering the sum (24) of the length (22) of the encrypted user data, which correspond to the second part, and the length of the third part of the unencrypted user data (18) in the start block (12).

6. A method for playing back an encrypted multimedia data stream (10), which has a start block (12) and a user data block (14), where a start section (20) of the user data block (14), which follows the start block (12), contains unencrypted user data and where a further section (16) of the user data block (14) contains encrypted user data, where the start block (12) contains information which is needed to play back the start section (20) of the user data block (14) and where the start block (12) contains information which is not needed to play back the unencrypted start section (20) of the user data block (14), comprising the following steps:

processing (110) the information of the start block (12)

which is needed to play back the start section (20) of the user data block (14); and

playing back (112) the unencrypted start section (20) of the user data block (14).

7. A method according to claim 6, which also includes the following steps:

processing (114) the information of the start block (12) which is not needed to play back the unencrypted start section (20);

decrypting the further section (16) of the user data block (14) using the processed information of the start block (12); and

playing back (118) the encrypted user data of the further section (16) of the user data block (14).

8. A method according to claim 7, wherein the step of processing (114) the information of the start block (12) which is not needed to play back the unencrypted start section (20) is performed essentially concurrently with the playing back (112) of the unencrypted start section (20).
9. A method according to one of the claims 6 to 8, wherein the length (22) of the unencrypted start section (20) of the user data block (14) is between 1 and 60 seconds.
10. A method according to one of the claims 6 to 9, wherein the user data to be encrypted are coded and wherein the information which is needed for playing back contains an

entry (72) specifying the type of coding/decoding method.

11. A method according to one of the preceding claims, wherein the user data are audio and/or video data.
12. A device for generating an encrypted user data stream (10), which has a start block (12) and a user data block (14), comprising:

a unit for generating (100) the start block (12); and

a unit for generating (102, 104, 106) the user data block (14), with the following features:

a unit for using (102) a first part of the user data to be encrypted as start section (20) for the user data block (14), the start section (20) being unencrypted;

a unit for encrypting (104) a second part of user data to be encrypted which follow the first part; and

a unit for appending (106) the encrypted user data (16) to the unencrypted start section (20).

13. A device for playing back an encrypted user data stream (10), which has a start block (12) and a user data block (14), where a start section (20) of the user data block (14), which follows the start block (12), contains unencrypted user data and where a further section (16) of the user data block (14) contains encrypted user data, where the start block (12) contains information which is needed to play back the start section (20) of the user data block (14) and where the start block (12) contains information which is not needed to play back the unencrypted start section (20) of the user data block (14), compris-

ing:

a unit for processing (110) the information of the start block (12) which is needed to play back the start section (20) of the user data block (14); and

a unit for playing back (112) the unencrypted start section (20) of the user data block (14).

14. A device according to claim 13, which further comprises:

a unit for processing (114) the information of the start block (12) which is not needed to play back the unencrypted start section (20);

a unit for decrypting the further section (16) of the user data block (14) using the processed information of the start block (12); and

a unit for playing back (118) the encrypted user data of the further section (16) of the user data block (14).

15. A device according to claim 14, wherein the unit for processing (114) the information of the start block (12) which is not needed to play back the unencrypted start section (20) is designed to be operated essentially concurrently to the unit for playing back (112) the unencrypted start section (20).
16. A device according to claim 13 which is implemented as a stereo system, hifi unit, solid state player, a playback unit with a hard disk or CD ROM, or a computer.
17. A device according to one of the claims 12 to 16, wherein the user data are audio and/or video data.

**Method and Device for Generating an Encrypted User Data Stream
and Method and Device for Playing Back an Encrypted User Data
Stream**

Abstract

In a method for generating an encrypted multimedia data stream a start block (12) and then a user data block (14) are generated. The start section (20) of the user data block contains unencrypted user data and is followed by encrypted user data (16). In this way a preview or prelisten function is implemented in a simple manner. In addition, a playback device can already play back the unencrypted start section (20) while the whole start block is being processed so as to obtain a multimedia data key for generating hash totals, etc. This parallel processing makes it possible to use playback devices with limited storage and processing resources without having to accept excessively long delays.

- 1/4 -

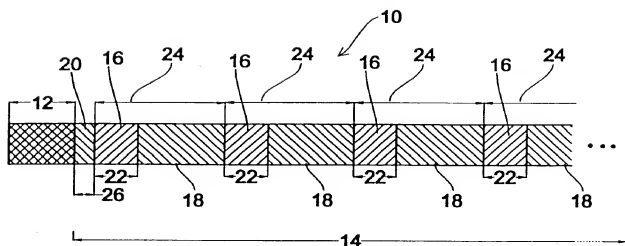


Fig. 1

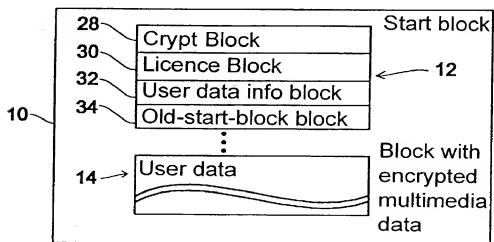


Fig. 2

- 2/4 -

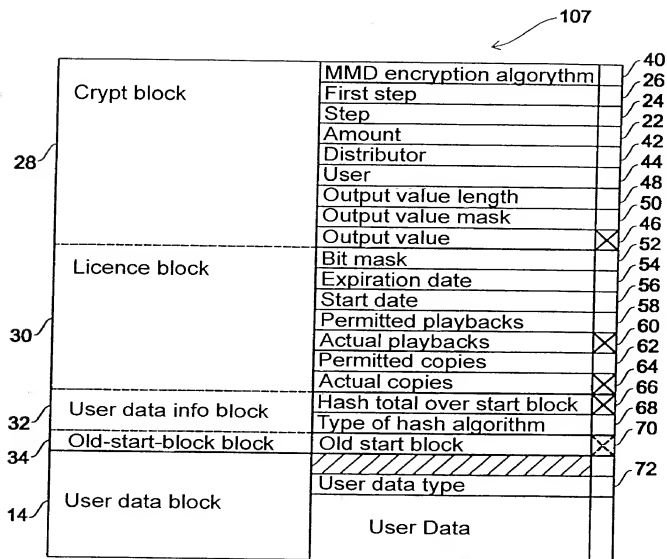


Fig. 3

09/913695

- 3/4 -

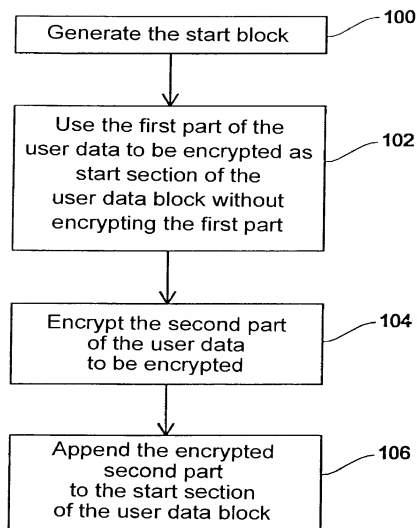


Fig. 4

- 4/4 -

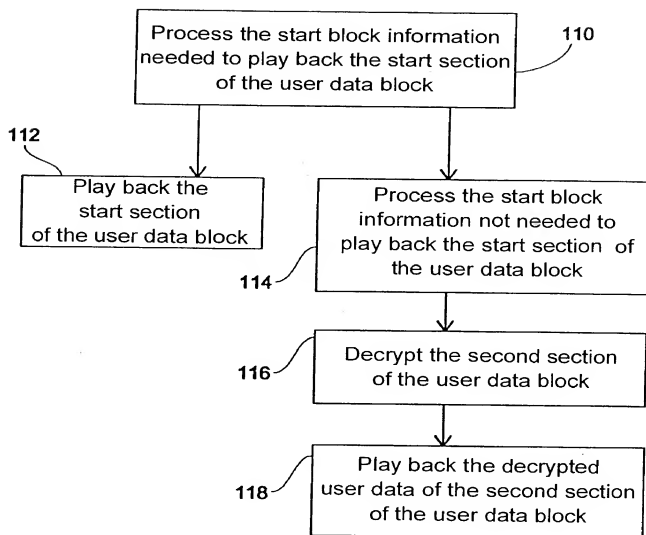


Fig. 5

09913695 09/913695

531 Rec'd PC 16 AUG 2001

National Phase of PCT/EP99/09977 in U.S.A.

Title: Method and Device for Generating an Encrypted User
Data Stream and Method and Device for Playing Back an
Encrypted User Data Stream

Applicants: RUMP, Niels et al.

Annotated copy of Final version of PCT/EP99/09977

4/PRTS

09913695.080202

09/913695

531 Rec'd PCT

16 AUG 2001

**Method and Device for Generating an Encrypted User Data Stream
and Method and Device for Playing Back an Encrypted User Data
Stream**

Field of the Invention

The present invention relates to the encrypting and decrypting of user data and in particular to the handling of encrypted user data streams with a start block and a user data block.

Background of the Invention and Prior Art

With the appearance of telecommunication networks and in particular because of the widespread use of personal computers capable of handling multimedia data and, more recently, also of so-called solid state players, a need has arisen to commercially exploit digital multimedia data, such as digital audio data and/or digital video data. The telecommunication networks might be e.g. analog telephone lines, digital telephone lines, such as ISDN, or the internet. Among commercial suppliers of multimedia products there is the need to sell or hire out multimedia data within a framework where a customer can select a particular product from a particular catalogue at any time, which product can then, of course, only be used by the customer who has paid for it.

In contrast to known encrypted television programs, such as those from the television channel Premiere, where the transmitted data are encrypted identically for all the users who have acquired a suitable decrypting device by paying a certain charge, the objective of the present invention is to provide methods and devices which offer an individual, customer-specific and secure encrypting and decrypting of multimedia

data. In contrast to the cited television channels, which provide a fixed program which the customer must accept as a package, the methods and devices of the present invention allow the customer maximum flexibility, i.e. he only has to pay for those products which he actually wishes to use.

DE 196 25 635 C1 describes methods and devices for encrypting and decrypting multimedia data where the multimedia data are in the form of an encrypted multimedia file with a definition data block and a user data block. Parts of the definition data block and parts at least of the user data block are encrypted with different keys and symmetric encrypting methods are chiefly used.

An advantage of symmetric encrypting methods is that they are relatively quick. On the other hand the user who wishes to decrypt the file needs the same key as the provider or supplier, e.g. Deutsche Telekom, who has encrypted the multimedia data, in order to sell them to the customer. Thus both the provider and the user, i.e. the customer, have one table with a plurality of possible symmetric encryption algorithms, such as DES or Blowfish, and another table for possible keys. The provider generates an entry in the definition data block of the multimedia data which the user then uses to access his key table so as to select the correct key for decrypting.

In response to the rapidly increasing deployment of the MP3 standard, so-called solid state players for decrypting and playing back multimedia data have appeared on the market. These players are meant to be very inexpensive, so they are restricted as to memory and computing power. In contrast to personal computers, which have resources far in excess of those needed for the decrypting of multimedia data, solid state players or stereo systems or car hifi units must be cheap to buy if they are to be successful in a very competi-

tive market. These devices must therefore be designed to decrypt multimedia data and play back the decrypted data using the minimum possible computing power and memory.

A disadvantage of the encrypting and decrypting concept in DE 196 25 635 C1 is the fact that the whole of the definition data block has to be processed before it is possible to start decrypting the user data block, decoding the decrypted user data block and, finally, playing back the decrypted decoded user data block.

This becomes a particular problem if the processing of the definition data block in a decrypting device entails substantial computing operations, e.g. calculating a hash total or a fingerprint of the start block. The situation could become even more serious if the decrypting device has only limited storage and processing resources. However, limited storage and processing resources are just what playback devices, in particular solid state players, should have if they are to be marketable in an inexpensive form.

A further disadvantage of the known encrypting and decrypting concept is the fact that a simple preview or prelisten function poses a problem. If the multimedia data are video data, it is sometimes desirable to be able to look at the first, say, 10 or 20 seconds, either to provide a basis for deciding whether to purchase the piece being offered or so as to make it possible to identify a particular piece. If the multimedia data are audio data, there is a need to be able to "listen into" a piece, i.e. to listen to the first, say, 10 or 20 seconds before deciding whether the piece should be purchased or so as to identify the piece.

Summary of the Invention

It is the object of the present invention to provide a concept for generating and playing back encrypted multimedia data streams which manages to do so with moderate storage and processing resources and which also permits an efficient implementation of a preview or prelisten function.

In accordance with a first aspect of the invention, this object is achieved by a method for generating an encrypted user data stream, which has a start block and a user data block, comprising the following steps: generating the start block; and generating the user data block by means of the following substeps: using a first part of the user data to be encrypted as start section for the user data block, the start section being unencrypted; encrypting a second part of user data to be encrypted which follow the first part; and appending the encrypted user data to the unencrypted start section.

In accordance with a second aspect of the invention, this object is achieved by a method for playing back an encrypted multimedia data stream, which has a start block and a user data block, where a start section of the user data block, which follows the start block, contains unencrypted user data and where a further section of the user data block contains encrypted user data, where the start block contains information which is needed to play back the start section of the user data block and where the start block contains information which is not needed to play back the unencrypted start section of the user data block, comprising the following steps: processing the information of the start block which is needed to play back the start section of the user data block; and playing back the unencrypted start section of the user data block.

In accordance with a third aspect of the invention, this object is achieved by a device for generating an encrypted user data stream, which has a start block and a user data block, comprising: a unit for generating the start block; and a unit for generating the user data block, comprising: a unit for using a first part of the user data to be encrypted as start section for the user data block, the start section being unencrypted; a unit for encrypting a second part of user data to be encrypted which follow the first part; and a unit for appending the encrypted user data to the unencrypted start section.

In accordance with a fourth aspect of the invention, this object is achieved by a device for playing back an encrypted user data stream, which has a start block and a user data block, where a start section of the user data block, which follows the start block, contains unencrypted user data and where a further section of the user data block contains encrypted user data, where the start block contains information which is needed to play back the start section of the user data block and where the start block contains information which is not needed to play back the unencrypted start section of the user data block, comprising: a unit for processing the information of the start block which is needed to play back the start section of the user data block; and a unit for playing back the unencrypted start section of the user data block.

The present invention is based on the finding that the concept that the user data are encrypted right from the start must be abandoned. In the prior art the aspiration was always to encrypt the user data right from the start in order to protect the whole user data block, and especially the initial part of it, from unauthorized access.

It should be noted that while user data generally refers to multimedia data, i.e. audio data, video data or a combination of audio and video data, it also includes e.g. text data. On the grounds of expediency, however, the subject matter of the present invention will be explained in terms of multimedia data. It is, however, apparent that all types of user data for which there is a need for encryption can be processed by the devices and methods of the present invention.

It was discovered, however, that the delay arising from the processing of the start block can become significant, especially when this involves complex operations such as forming hash totals, the more so when playback devices with limited storage and processing resources are to be used.

It was also discovered that the demands made on the processing capacity of a processor with limited processing power are particularly high when processing the start block but are lower when decrypting, decoding and playing back the decrypted decoded multimedia data. This means that a relatively high processing power must be provided only for the processing of the start block and that this is no longer fully exploited when decrypting, decoding and playing back the data stream. It should be noted that the security of an encrypted multimedia data stream is essentially ensured by the start block, i.e. that it is always advisable to employ a relatively high computing power to process this block in order to achieve secure concepts. For this reason it is not desirable that the processing of the start block in general should be simplified so as to reduce the delay arising from the processing of the start block.

According to the present invention a certain section which commences at the beginning of the multimedia data to be encrypted, i.e. at the beginning of a user data block, and which

terminates after a predetermined duration of the multimedia data to be encrypted, i.e. a first part of the multimedia data to be encrypted, is not therefore encrypted but is written unencrypted into a start section of the user data block of the encrypted multimedia data. Encryption commences only with the multimedia data which follow the first part, these being encrypted in a suitable manner and appended to the start section of the user data block. This means that the first part of a multimedia data item, normally within the range from 5 to 20 seconds, is freely accessible. The demands made on the processor in order to play back this first part are minimal since no hash totals have to be calculated and no encrypted multimedia key has to be decrypted, etc. Furthermore, at this stage it is not absolutely necessary to process elaborate licence data relating to the authorized use of the multimedia data stream. A playback device will therefore be able to play back the first part of the multimedia data without any significant delay. Accordingly, it is already possible to achieve an effective preview or prelisten function in a simple and efficient manner.

Providing an unencrypted start section of the user data block brings further significant advantages, however, if the decrypting devices have only limited storage and processing resources, which is very much the case for solid state players, which must be put on the market at the lowest possible price. If multimedia data to be encrypted are coded with some sort of MPEG method, for example, a playback device simply has to decode and play back the multimedia data in order to be able to play back the start section of the user data block. The playback device thus has processing resources available during the decoding and playback phase with which it can fully process the start block itself while the start section of the user data block, which is unencrypted, is being played back. It can then decrypt, decode and play back the subsequent encrypted part of the user data block.

The provision according to the present invention of an unencrypted start section of the user data block therefore makes it possible to allocate the necessary storage and processing resources in such a way that, even with playback devices with limited resources, it is possible to decrypt, decode and play back multimedia data without excessively long delay.

Brief Description of the Drawings

Preferred embodiments of the present invention are described in detail below making reference to the enclosed drawings, in which

- Fig. 1 shows a multimedia data stream, which can be generated according to the present invention;
- Fig. 2 shows a detailed representation of the start block and of the user data block of the encrypted multimedia data stream;
- Fig. 3 shows a selection of some of the entries in the individual subblocks of the start block;
- Fig. 4 shows a flowchart of the method of generating an encrypted multimedia data stream according to the present invention; and
- Fig. 5 shows a flowchart of the method of playing back an encrypted multimedia data stream according to the present invention.

Detailed Description of the Preferred Embodiments

Fig. 1 shows an encrypted multimedia data stream 10, which has a start block or header 12 and a user data block 14, i.e. a block with encrypted multimedia data. The user data block 14 encompasses encrypted sections 16 and unencrypted sections 18 between the encrypted sections 16. Furthermore, a multimedia data stream which can be generated according to the present invention also has a further unencrypted section 20, which follows the start block 12 and precedes an encrypted section 16.

Normally the multimedia data to be encrypted are coded in some way, e.g. according to an MPEG standard such as MPEG-2 AAC, MPEG-4 AAC or MPEG layer 3. It suffices therefore to encrypt just certain sections of the multimedia data to be encrypted. This leads to a considerably reduced processing effort both on the part of the provider, who encrypts the data, and on the part of the customer, who must decrypt the data again. Apart from this, as a consequence of the only partial encryption of the multimedia data the pleasure which a user who utilizes only the unencrypted multimedia data enjoys, whether listening or viewing, is severely impaired due to the encrypted blocks, which appear at regular intervals.

Although Fig. 1 shows an encrypted multimedia data stream wherein the start block 12 is at the start of the encrypted multimedia data stream, this arrangement of start block and user data block should not be taken to relate to the transmission of the encrypted multimedia data stream. The expression "start block" is merely meant to indicate that a decrypting device which wishes to decrypt the encrypted multimedia data stream first requires at least parts of the start block before the multimedia data themselves can be decrypted. Depending on the transmission medium, the start block could also be located

somewhere within the user data block or could well be received after certain parts of the user data block, e.g. in the case of a packet-oriented transmission of the multimedia data stream where different packets, one of which may contain the start block and some other may contain part of the user data block, are transmitted over different physical transmission paths and where there is absolutely no need for the received sequence to correspond to the transmitted sequence. In this case a decrypting device must, however, be capable of storing the received packets and rearranging them in such a way that information can be extracted from the start block so as to be able to start decrypting. The encrypted multimedia data stream might also take the form of a file or it might also take the form of an actual data stream, e.g. in the case of a live transmission of a multimedia event. This application will feature particularly in the case of digital user-selective broadcasting.

The length of an encrypted section 16 is represented by a value Amount 22, while the interval in the encrypted multimedia data stream from the start of an encrypted section 16 to the start of the next encrypted section 16 is indicated by Step 24. The length of the further unencrypted section 20 is given by a value First step 26.

These values 22, 24 and 26 are, of course, needed for the correct decryption of the multimedia data in a decrypting device, which is why these values must be entered in the start block 12, as will be explained later.

It should be noted, however, that the relative sizes of the values 22 and 24 can be variable. One of the possibilities is that the length of the unencrypted section 18 is zero, i.e. that encryption is complete.

Fig. 2 shows a more detailed representation of the encrypted multimedia data stream 10, which comprises the start block 12 and the user data block 14. The start block 12 is subdivided into a number of subblocks, which will be described individually with especial reference to Fig. 3. Attention is drawn to the fact that the number and function of the subblocks can be expanded without restriction. Just some of these subblocks of the start block 12 are therefore shown as an example in Fig. 2. As shown in Fig. 2 the start block 12 includes a so-called crypt block 28, which, roughly speaking, contains information which is relevant to the encryption of the multimedia data. The start block 12 also has a so-called licence block 30, which contains data relating to the way in which a user can or may utilize the encrypted multimedia data stream. The start block 12 also includes a user data info block 32, which can include information relating to the user data block 14 and general information on the start block 12 itself. In addition, the start block 12 may also have an old-start-block block 34, which permits a so-called recursive start block structure. This block enables the user who has not only a decrypting device but also an encrypting device to reformat an encrypted multimedia data stream for other playback devices in his possession without losing or modifying the start block information originally supplied by the distributor. Depending on the application, further subblocks, e.g. an IP information block (IP = Intellectual Property) according to ISO/IEC 14496-1, MPEG-4, Systems, 1998, which contains copyright information, can be included in the start block 12.

As is customary in the field of technology, each block can be designed to have an internal block structure, which first requires a block identifier, then contains the length of the subblock, and then, finally, presents the block user data as such. This increases the flexibility of the encrypted multimedia data stream and in particular that of the start block of

the encrypted multimedia data stream in that new demands can be responded to by adding further subblocks and omitting existing subblocks.

Fig. 3 provides an overview of the block user data of the individual subblocks shown in Fig. 2.

The crypt block 28 is considered first. This contains an entry for a multimedia data encryption algorithm 40 which identifies the symmetric encryption algorithm which has been used to encrypt the multimedia data in a preferred embodiment of the present invention. The entry 40 may well be an index for a table such that a decrypting device having read the entry 40 is able to select from among a plurality of encryption algorithms the same encryption algorithm at that used by the encrypting device. The crypt block 28 also includes the entry First step 26, the entry Step 24 and the entry Amount 22, which have already been referred to in connection with Fig. 1. These entries in the start block enable a decrypting device to subdivide an encrypted multimedia data stream appropriately so as to be able to perform decryption correctly.

The crypt block 28 also contains an entry for the distributor or provider or supplier 42 which is a code for the distributor who has generated the encrypted multimedia data stream. An entry User 44 identifies the user who has received the encrypted multimedia data stream in some way or other from the distributor identified by the entry 42. One possible use for these identifiers is to make the user identification device-specific. The entry User would then contain the serial number of a PC, a laptop, a car hifi device, a home stereo system, etc., which only permits playback on the specific device. To further improve the flexibility and/or security, instead of using the serial number, which has a different structure from one manufacturer to another, but which could be duplicated by

chance, a special identification, e.g. a logical coupling of the size of the fixed disk with the processor number etc. in the case of a PC, could be used instead.

An entry 46 contains an output value, which will be discussed in more detail later. This output value represents, generally speaking, an encrypted version of the multimedia data key, which is needed, in conjunction with the multimedia data encryption algorithm identified by the entry 40, in order to correctly decrypt the encrypted multimedia data (sections 16 in Fig. 1) in the user data block 14. To ensure adequate flexibility for future applications, the two entries Output value length 48 and Output value mask 50 have been provided. The entry Output value length 48 indicates the actual length of the output value 46. However, to achieve a flexible start block format more bytes are provided therein for the output value than an output value can actually have at the present time. The output value mask 50 thus indicates how a shorter output value is distributed over a longer output value space. If the output value length is e.g. half as big as the space available for the output value, the output value mask could be so constituted that the first half of the output value mask is set and the second half is not set. The output value would then simply be entered in the space allocated by the syntax for the start block and occupy the first half of this space while the other half is ignored due to the output value mask 50.

The licence block 30 of the start block 12 will now be considered. This includes an entry Bit mask 52. This entry can contain certain special information for playing back or for the general mode of using the encrypted multimedia data. In particular, a decrypting device could be informed in this way whether or not the user data can be played back locally. Furthermore, it could be signaled here whether the challenge-

response method described in the German Patent DE 196 25 635 C1 cited earlier and which permits efficient database access has been used for encryption.

An entry Expiration date 54 indicates the date on which permission to decrypt the encrypted multimedia data stream expires. A decrypting device will check the entry Expiration date 54 and compare it with a built-in timer. If the expiration date has been passed, the decrypting device will no longer perform a decryption of the encrypted multimedia data stream. This enables a provider to supply encrypted multimedia data for a limited time period, offering the advantage of a much greater flexibility in the management of the data and in pricing policy. This flexibility is further supported by an entry Start date 56, which specifies when decryption of a encrypted multimedia file may commence. A decrypting device will compare the entry Start date with its own built-in clock and will only start decrypting the encrypted multimedia data when the actual time is later than that specified by the start date 56.

An entry Permitted playbacks 58 specifies how often the encrypted multimedia data stream may be decrypted, i.e. played back. This further increases the flexibility of the provider in that he only permits a certain number of playbacks, e.g. in return for a certain sum which is less than that which would be demanded for the unrestricted use of the encrypted multimedia data stream.

To verify or support the entry Permitted playbacks 58 the licence block 30 has another entry Actual playbacks 60, which could e.g. be incremented by one after each decryption of the encrypted multimedia data stream. A decrypting device will thus always check whether the entry Actual playbacks is less than the entry Permitted playbacks. If this is so, the multi-

media data will be decrypted. If not, no further decryption takes place.

The entries Permitted copies 62 and Actual copies 64 are analogues of the entries 58 and 60. By means of the two entries 62 and 64 it is ensured that the user of the multimedia data only copies them as often as he is allowed to do so by the provider or as often as is warranted by the cost of buying the multimedia data. By means of the entries 58 to 64 an effective copyright protection is guaranteed and it is possible to discriminate between private users and commercial users, e.g. by setting the entries Permitted playbacks 58 and Permitted copies 62 to a small value.

Licensing might e.g. be on the basis that a certain number of copies (entry 62) of the original is permitted while no copies of a copy are allowed. The start block of a copy would then, in contrast to the start block of the original, have a zero in the entry Permitted copies, meaning that this copy will not be copied again by a correctly functioning encrypting/decrypting device.

In the example of a multimedia data protection protocol (MMP; MMP = Multimedia Protection Protocol) shown here, the start block 12 also contains a user data information block 32 which has just two block user data entries 66 and 68, the entry 66 containing a hash total over the whole start block and the entry 68 identifying the type of hash algorithm which has been used to generate the hash total over the whole start block.

Among the publications which are useful in this connection is the technical book "Applied Cryptography", Second Edition, John Wiley & Sons, Inc. By Bruce Schneier (ISBN 0 471-11709-9) which contains a comprehensive treatment of symmetric encryp-

tion algorithms, asymmetric encryption algorithms and hash algorithms.

Finally the start block 12 includes the old-start-block block 34, which in addition to the synchronization information, which is not shown in Fig. 3, contains the entry Old start block 70. If a user performs his own encryption and thus generates a new start block 12, the old start block from the provider can be preserved in the entry Old start block 70 so as not to lose any important information that the provider has written into the start block. This might include copyright information (IP information block), previous user information and distributor information, which make it possible to trace back a multimedia file, which e.g. has been decrypted/encrypted several times by various devices, to the original supplier while preserving copyright information. In this way it is possible to check at all times whether an encrypted multimedia file has been acquired legally or illegally.

It is obvious that the sequence of steps in Fig. 5 can be varied in the same way as explained below with reference to Fig. 4.

Fig. 4 shows a flowchart of the method according to the present invention for generating an encrypted multimedia data stream. In a step 100 the start block 12 is generated. Then, in a step 102, the first part of the multimedia data to be encrypted is used as the start section of the user data block 14, but this first part itself is not encrypted. The start section thus forms the further unencrypted section 20 of Fig. 1, whose length is specified in the entry First step 26 in the start block. The second part of the multimedia data to be encrypted is then encrypted in a step 104 to generate the encrypted section 16 which follows the unencrypted section 20

(Fig. 1). To produce a simple encrypted multimedia data stream, the encrypted second part is appended to the start section of the user data block (step 106), so that the encrypted multimedia data stream 10 contains the start block 12, the start section 20 and the encrypted second part 16. The encrypted multimedia data stream can now be extended as desired by generating another unencrypted section 18, an encrypted section 16, etc. and writing them into the user data block 14.

From Fig. 4 it can be seen that there is no fixed sequence for the steps 100 to 106. The start block could also be generated after completion of the user data block and placed at the head of the user data block using a block multiplexer. Alternatively, the second part of the multimedia data to be encrypted could be encrypted (step 104) before the first part is written into the data block since the entry First step 26 defines precisely the point, i.e. the bit position, in the data block 14 at which the encrypted second part must start to be entered. What is important here is simply that the unencrypted start section 20 of the user data block 14 should be placed immediately after the start block 12. It should be emphasized again at this point that the sequence of start block, unencrypted start section and encrypted second part (i.e. 12, 20, 16) described here simply describes the sequence in which the multimedia data stream must be arranged in the playback device so as to exploit the advantages of the present invention. This sequence has no effect on the transmission of the encrypted multimedia data stream. This becomes particularly apparent when a packet-oriented transmission is used. A packet for the start block, a packet for the start section and a packet for the encrypted second part could be transmitted over different paths from a transmitter to a receiver in such a way that the start section arrives first, followed by the encrypted second part and finally the start block. In this case, of course,

the playback device must be capable of rearranging the three packets, as has already been described.

Fig. 5 shows a flowchart of the method according to the present invention for playing back the encrypted multimedia data stream 10 comprising the start block 12, the unencrypted start section 20 of the user data block 14 and the encrypted second part 16 of the user data block 14. According to the present invention only the information of the start block 12 which is absolutely necessary for playing back the unencrypted start section of the user data block 14 (step 110) is initially processed in the playback device.

Subsequently the unencrypted start section 20 of the user data block 14 can be played back with minimal delay (step 112). In this way a simple and efficient preview or prelisten function is achieved. Playing back the start section of the user data block (step 112) will not normally require the full processing power of the playback device. Thus the playback device can, while playing back the start section, also process essentially concurrently the other information of the start block 12, i.e. the information which is not needed to play back the start section of the user data block (step 114). Once the start block 12 has been processed, the playback device will then be able to decrypt the encrypted multimedia data in the first encrypted section 16, i.e. the encrypted second part of the user data block 14 (step 116), thus enabling it to then play back the decrypted multimedia data of the second section (step 118).

The information which is absolutely necessary for playing back the unencrypted start section 20 will now be discussed making reference to Fig. 3. Among the information which is absolutely necessary are the general block identification information and block length information, which are not shown in Fig. 3, which

enable a playback device to correctly locate where the necessary information is to be found in the start block. If the multimedia data are coded in some way, as is usually the case, e.g. according to an MPEG method, the playback device will have to extract this information from the start block 12 in step 110 (Fig. 5). In the table in Fig. 3 this information is contained in the entry User data type of the user data block 14. The playback device then knows that the unencrypted data in the start section 20 of the user data block 14 are coded in e.g. MPEG layer 3 format (MP3), so that the playback device can then decode and play back the unencrypted multimedia data (step 112). While the start section 20 is being played back the device is now able to process all the relatively complicated additional data of the start section, such as the data in the crypt block 28, in the licence block 30 and in the user data information block 32, which in particular contains a relatively complex hash total /digital signature over the start block (entry 66). Another complicated operation is that of decrypting the multimedia data key from the output value (entry 46) so as to be able to decrypt the encrypted sections 16 (Fig. 1) of the encrypted multimedia data stream.

It is possible to specify whether or not the entries Distributor 42 and User 44 should also belong to the necessary information for playing back the unencrypted start section 20. If so, the preview or prelisten function is only available for a particular user or for the subscribers of a particular distributor. This means that, via the very simple and uncomplicated implementation of the preview or prelisten function, a distributor can send an encrypted multimedia file to a special user or to all his subscription users, who can then listen to or view an extract of e.g. 1 second's to 1 minute's duration, i.e. the unencrypted start section 20. If a user finds this offering to his taste he can then decide to pay for the whole

encrypted multimedia data stream. This facility also enables individual items to be identified in a simple manner.

In this case it is not necessary to perform the steps 114, 116 and 118. It should be noted that it is in fact not possible to perform these steps in this case, since the user may not yet possess the information as to how the output value 46 must be decrypted so as to obtain the multimedia data key enabling the encrypted multimedia data in the encrypted sections 16 to be decrypted. Should a user decide to purchase after his appetite has been whetted by the preview or prelisten function, all the distributor has to do is to enable the user to decrypt the output value.

Providing an unencrypted start section in the user data block thus enables the preview or prelisten function to be offered in a simple way and also makes it possible to use processors with limited storage or processing resources without having to put up with significant delays resulting from the processing of the whole start block.

Claims

1. A method for generating an encrypted user data stream, which has a start block and a user data block, comprising the following steps:

generating the start block; and

generating the user data block by means of the following substeps:

using a first part of the user data to be encrypted as start section for the user data block, the start section being unencrypted;

encrypting a second part of user data to be encrypted which follow the first part; and

appending the encrypted user data to the unencrypted start section.

2. A method according to claim 1, wherein the step of generating the start block includes the following substep:

entering the length of the start section in the start block.

3. A method according to claim 1, wherein the second part does not comprise all the user data to be encrypted and wherein the step of generating the user data block includes the following substep:

appending a third part of user data to be encrypted, which follow the second part, to the encrypted user data

of the second part, the user data of the third part being unencrypted.

4. A method according to claim 1, wherein the step of generating the start block includes the following substep:

entering the length of the encrypted multimedia data, which correspond to the user data of the second part which are to be encrypted, in the start block.

5. A method according to claim 3, wherein the step of generating the start block also includes the following substep:

entering the sum of the length of the encrypted user data, which correspond to the second part, and the length of the third part of the unencrypted user data in the start block.

6. A method for playing back an encrypted multimedia data stream, which has a start block and a user data block, where a start section of the user data block, which follows the start block, contains unencrypted user data and where a further section of the user data block contains encrypted user data, where the start block contains information which is needed to play back the start section of the user data block and where the start block contains information which is not needed to play back the unencrypted start section of the user data block, comprising the following steps:

processing the information of the start block which is needed to play back the start section of the user data block; and

playing back the unencrypted start section of the user data block.

7. A method according to claim 6, which also includes the following steps:

processing the information of the start block which is not needed to play back the unencrypted start section;

decrypting the further section of the user data block using the processed information of the start block; and

playing back the encrypted user data of the further section of the user data block.

8. A method according to claim 7, wherein the step of processing the information of the start block which is not needed to play back the unencrypted start section is performed essentially concurrently with the playing back of the unencrypted start section.
9. A method according to claim 6, wherein the length of the unencrypted start section of the user data block is between 1 and 60 seconds.
10. A method according to claim 6, wherein the user data to be encrypted are coded and wherein the information which is needed for playing back contains an entry specifying the type of coding/decoding method.
11. A method according to claim 1, wherein the user data are audio and/or video data.
12. A device for generating an encrypted user data stream, which has a start block and a user data block, compris-

ing:

a unit for generating the start block; and

a unit for generating the user data block, with the following features:

a unit for using a first part of the user data to be encrypted as start section for the user data block, the start section being unencrypted;

a unit for encrypting a second part of user data to be encrypted which follow the first part; and

a unit for appending the encrypted user data to the unencrypted start section.

13. A device for playing back an encrypted user data stream, which has a start block and a user data block, where a start section of the user data block, which follows the start block, contains unencrypted user data and where a further section of the user data block contains encrypted user data, where the start block contains information which is needed to play back the start section of the user data block and where the start block contains information which is not needed to play back the unencrypted start section of the user data block, comprising:

a unit for processing the information of the start block which is needed to play back the start section of the user data block; and

a unit for playing back the unencrypted start section of the user data block.

14. A device according to claim 13, which further comprises:

a unit for processing the information of the start block which is not needed to play back the unencrypted start section;

a unit for decrypting the further section of the user data block using the processed information of the start block; and

a unit for playing back the encrypted user data of the further section of the user data block.

15. A device according to claim 14, wherein the unit for processing the information of the start block which is not needed to play back the unencrypted start section is designed to be operated essentially concurrently to the unit for playing back the unencrypted start section.

16. A device according to claim 13 which is implemented as a stereo system, hifi unit, solid state player, a playback unit with a hard disk or CD ROM, or a computer.

17. A device according to claim 12, wherein the user data are audio and/or video data.

**Method and Device for Generating an Encrypted User Data Stream
and Method and Device for Playing Back an Encrypted User Data
Stream**

Abstract

In a method for generating an encrypted multimedia data stream a start block and then a user data block are generated. The start section of the user data block contains unencrypted user data and is followed by encrypted user data. In this way a preview or prelisten function is implemented in a simple manner. In addition, a playback device can already play back the unencrypted start section while the whole start block is being processed so as to obtain a multimedia data key for generating hash totals, etc. This parallel processing makes it possible to use playback devices with limited storage and processing resources without having to accept excessively long delays.

09913695 080302
09/913695
31 Rec'd PCT/PTO 16 AUG 2001

National Phase of PCT/EP99/09977 in U.S.A.

Title: Method and Device for Generating an Encrypted User
Data Stream and Method and Device for Playing Back an
Encrypted User Data Stream

Applicants: RUMP, Niels et al.

Translation of PCT Application PCT/EP99/09977
as originally filed

09/913695

531 Rec'd PCT.

16 AUG 2001

Method and Device for Generating an Encrypted User Data Stream
and Method and Device for Playing Back an Encrypted User Data
Stream

[Description]

Field of the Invention

The present invention relates to the encrypting and decrypting of user data and in particular to the handling of encrypted user data streams with a start block and a user data block.

Background of the Invention and Prior Art

With the appearance of telecommunication networks and in particular because of the widespread use of personal computers capable of handling multimedia data and, more recently, also of so-called solid state players, a need has arisen to commercially exploit digital multimedia data, such as digital audio data and/or digital video data. The telecommunication networks might be e.g. analog telephone lines, digital telephone lines, such as ISDN, or the internet. Among commercial suppliers of multimedia products there is the need to sell or hire out multimedia data within a framework where a customer can select a particular product from a particular catalogue at any time, which product can then, of course, only be used by the customer who has paid for it.

In contrast to known encrypted television programs, such as those from the television channel Premiere, where the transmitted data are encrypted identically for all the users who have acquired a suitable decrypting device by paying a certain charge, the objective of the present invention is to provide methods and devices which offer an individual, customer-

specific and secure encrypting and decrypting of multimedia data. In contrast to the cited television channels, which provide a fixed program which the customer must accept as a package, the methods and devices of the present invention allow the customer maximum flexibility, i.e. he only has to pay for those products which he actually wishes to use.

DE 196 25 635 C1 describes methods and devices for encrypting and decrypting multimedia data where the multimedia data are in the form of an encrypted multimedia file with a definition data block and a user data block. Parts of the definition data block and parts at least of the user data block are encrypted with different keys and symmetric encrypting methods are chiefly used.

An advantage of symmetric encrypting methods is that they are relatively quick. On the other hand the user who wishes to decrypt the file needs the same key as the provider or supplier, e.g. Deutsche Telekom, who has encrypted the multimedia data, in order to sell them to the customer. Thus both the provider and the user, i.e. the customer, have one table with a plurality of possible symmetric encryption algorithms, such as DES or Blowfish, and another table for possible keys. The provider generates an entry in the definition data block of the multimedia data which the user then uses to access his key table so as to select the correct key for decrypting.

In response to the rapidly increasing deployment of the MP3 standard, so-called solid state players for decrypting and playing back multimedia data have appeared on the market. These players are meant to be very inexpensive, so they are restricted as to memory and computing power. In contrast to personal computers, which have resources far in excess of those needed for the decrypting of multimedia data, solid state players or stereo systems or car hifi units must be

cheap to buy if they are to be successful in a very competitive market. These devices must therefore be designed to decrypt multimedia data and play back the decrypted data using the minimum possible computing power and memory.

A disadvantage of the encrypting and decrypting concept in DE 196 25 635 C1 is the fact that the whole of the definition data block has to be processed before it is possible to start decrypting the user data block, decoding the decrypted user data block and, finally, playing back the decrypted decoded user data block.

This becomes a particular problem if the processing of the definition data block in a decrypting device entails substantial computing operations, e.g. calculating a hash total or a fingerprint of the start block. The situation could become even more serious if the decrypting device has only limited storage and processing resources. However, limited storage and processing resources are just what playback devices, in particular solid state players, should have if they are to be marketable in an inexpensive form.

A further disadvantage of the known encrypting and decrypting concept is the fact that a simple preview or prelisten function poses a problem. If the multimedia data are video data, it is sometimes desirable to be able to look at the first, say, 10 or 20 seconds, either to provide a basis for deciding whether to purchase the piece being offered or so as to make it possible to identify a particular piece. If the multimedia data are audio data, there is a need to be able to "listen into" a piece, i.e. to listen to the first, say, 10 or 20 seconds before deciding whether the piece should be purchased or so as to identify the piece.

Summary of the Invention

It is the object of the present invention to provide a concept for generating and playing back encrypted multimedia data streams which manages to do so with moderate storage and processing resources and which also permits an efficient implementation of a preview or prelisten function.

[This object is achieved by a method for generating an encrypted user data stream according to claim 1, by a method for playing back an encrypted user data stream according to claim 6, by a device for generating an encrypted user data stream according to claim 12 and by a device for playing back an encrypted user data stream according to claim 13.]

In accordance with a first aspect of the invention, this object is achieved by a method for generating an encrypted user data stream, which has a start block and a user data block, comprising the following steps: generating the start block; and generating the user data block by means of the following substeps: using a first part of the user data to be encrypted as start section for the user data block, the start section being unencrypted; encrypting a second part of user data to be encrypted which follow the first part; and appending the encrypted user data to the unencrypted start section.

In accordance with a second aspect of the invention, this object is achieved by a method for playing back an encrypted multimedia data stream, which has a start block and a user data block, where a start section of the user data block, which follows the start block, contains unencrypted user data and where a further section of the user data block contains encrypted user data, where the start block contains information which is needed to play back the start section of the user data block and where the start block contains information

which is not needed to play back the unencrypted start section of the user data block, comprising the following steps: processing the information of the start block which is needed to play back the start section of the user data block; and playing back the unencrypted start section of the user data block.

In accordance with a third aspect of the invention, this object is achieved by a device for generating an encrypted user data stream, which has a start block and a user data block, comprising: a unit for generating the start block; and a unit for generating the user data block, comprising: a unit for using a first part of the user data to be encrypted as start section for the user data block, the start section being unencrypted; a unit for encrypting a second part of user data to be encrypted which follow the first part; and a unit for appending the encrypted user data to the unencrypted start section.

In accordance with a fourth aspect of the invention, this object is achieved by a device for playing back an encrypted user data stream, which has a start block and a user data block, where a start section of the user data block, which follows the start block, contains unencrypted user data and where a further section of the user data block contains encrypted user data, where the start block contains information which is needed to play back the start section of the user data block and where the start block contains information which is not needed to play back the unencrypted start section of the user data block, comprising: a unit for processing the information of the start block which is needed to play back the start section of the user data block; and a unit for playing back the unencrypted start section of the user data block.

The present invention is based on the finding that the concept that the user data are encrypted right from the start must be

abandoned. In the prior art the aspiration was always to encrypt the user data right from the start in order to protect the whole user data block, and especially the initial part of it, from unauthorized access.

It should be noted that while user data generally refers to multimedia data, i.e. audio data, video data or a combination of audio and video data, it also includes e.g. text data. On the grounds of expediency, however, the subject matter of the present invention will be explained in terms of multimedia data. It is, however, apparent that all types of user data for which there is a need for encryption can be processed by the devices and methods of the present invention.

It was discovered, however, that the delay arising from the processing of the start block can become significant, especially when this involves complex operations such as forming hash totals, the more so when playback devices with limited storage and processing resources are to be used.

It was also discovered that the demands made on the processing capacity of a processor with limited processing power are particularly high when processing the start block but are lower when decrypting, decoding and playing back the decrypted decoded multimedia data. This means that a relatively high processing power must be provided only for the processing of the start block and that this is no longer fully exploited when decrypting, decoding and playing back the data stream. It should be noted that the security of an encrypted multimedia data stream is essentially ensured by the start block, i.e. that it is always advisable to employ a relatively high computing power to process this block in order to achieve secure concepts. For this reason it is not desirable that the processing of the start block in general should be simplified so

as to reduce the delay arising from the processing of the start block.

According to the present invention a certain section which commences at the beginning of the multimedia data to be encrypted, i.e. at the beginning of a user data block, and which terminates after a predetermined duration of the multimedia data to be encrypted, i.e. a first part of the multimedia data to be encrypted, is not therefore encrypted but is written unencrypted into a start section of the user data block of the encrypted multimedia data. Encryption commences only with the multimedia data which follow the first part, these being encrypted in a suitable manner and appended to the start section of the user data block. This means that the first part of a multimedia data item, normally within the range from 5 to 20 seconds, is freely accessible. The demands made on the processor in order to play back this first part are minimal since no hash totals have to be calculated and no encrypted multimedia key has to be decrypted, etc. Furthermore, at this stage it is not absolutely necessary to process elaborate licence data relating to the authorized use of the multimedia data stream. A playback device will therefore be able to play back the first part of the multimedia data without any significant delay. Accordingly, it is already possible to achieve an effective preview or prelisten function in a simple and efficient manner.

Providing an unencrypted start section of the user data block brings further significant advantages, however, if the decrypting devices have only limited storage and processing resources, which is very much the case for solid state players, which must be put on the market at the lowest possible price. If multimedia data to be encrypted are coded with some sort of MPEG method, for example, a playback device simply has to decode and play back the multimedia data in order to be able to play back the start section of the user data block. The play-

back device thus has processing resources available during the decoding and playback phase with which it can fully process the start block itself while the start section of the user data block, which is unencrypted, is being played back. It can then decrypt, decode and play back the subsequent encrypted part of the user data block.

The provision according to the present invention of an unencrypted start section of the user data block therefore makes it possible to allocate the necessary storage and processing resources in such a way that, even with playback devices with limited resources, it is possible to decrypt, decode and play back multimedia data without excessively long delay.

Brief Description of the Drawings

Preferred embodiments of the present invention are described in detail below making reference to the enclosed drawings, in which

- Fig. 1 shows a multimedia data stream, which can be generated according to the present invention;
- Fig. 2 shows a detailed representation of the start block and of the user data block of the encrypted multimedia data stream;
- Fig. 3 shows a selection of some of the entries in the individual subblocks of the start block;
- Fig. 4 shows a flowchart of the method of generating an encrypted multimedia data stream according to the present invention; and

Fig. 5 shows a flowchart of the method of playing back an encrypted multimedia data stream according to the present invention.

Detailed Description of the Preferred Embodiments

Fig. 1 shows an encrypted multimedia data stream 10, which has a start block or header 12 and a user data block 14, i.e. a block with encrypted multimedia data. The user data block 14 encompasses encrypted sections 16 and unencrypted sections 18 between the encrypted sections 16. Furthermore, a multimedia data stream which can be generated according to the present invention also has a further unencrypted section 20, which follows the start block 12 and precedes an encrypted section 16.

Normally the multimedia data to be encrypted are coded in some way, e.g. according to an MPEG standard such as MPEG-2 AAC, MPEG-4 AAC or MPEG layer 3. It suffices therefore to encrypt just certain sections of the multimedia data to be encrypted. This leads to a considerably reduced processing effort both on the part of the provider, who encrypts the data, and on the part of the customer, who must decrypt the data again. Apart from this, as a consequence of the only partial encryption of the multimedia data the pleasure which a user who utilizes only the unencrypted multimedia data enjoys, whether listening or viewing, is severely impaired due to the encrypted blocks, which appear at regular intervals.

Although Fig. 1 shows an encrypted multimedia data stream wherein the start block 12 is at the start of the encrypted multimedia data stream, this arrangement of start block and user data block should not be taken to relate to the transmission of the encrypted multimedia data stream. The expression

"start block" is merely meant to indicate that a decrypting device which wishes to decrypt the encrypted multimedia data stream first requires at least parts of the start block before the multimedia data themselves can be decrypted. Depending on the transmission medium, the start block could also be located somewhere within the user data block or could well be received after certain parts of the user data block, e.g. in the case of a packet-oriented transmission of the multimedia data stream where different packets, one of which may contain the start block and some other may contain part of the user data block, are transmitted over different physical transmission paths and where there is absolutely no need for the received sequence to correspond to the transmitted sequence. In this case a decrypting device must, however, be capable of storing the received packets and rearranging them in such a way that information can be extracted from the start block so as to be able to start decrypting. The encrypted multimedia data stream might also take the form of a file or it might also take the form of an actual data stream, e.g. in the case of a live transmission of a multimedia event. This application will feature particularly in the case of digital user-selective broadcasting.

The length of an encrypted section 16 is represented by a value Amount 22, while the interval in the encrypted multimedia data stream from the start of an encrypted section 16 to the start of the next encrypted section 16 is indicated by Step 24. The length of the further unencrypted section 20 is given by a value First step 26.

These values 22, 24 and 26 are, of course, needed for the correct decryption of the multimedia data in a decrypting device, which is why these values must be entered in the start block 12, as will be explained later.

It should be noted, however, that the relative sizes of the values 22 and 24 can be variable. One of the possibilities is that the length of the unencrypted section 18 is zero, i.e. that encryption is complete.

Fig. 2 shows a more detailed representation of the encrypted multimedia data stream 10, which comprises the start block 12 and the user data block 14. The start block 12 is subdivided into a number of subblocks, which will be described individually with especial reference to Fig. 3. Attention is drawn to the fact that the number and function of the subblocks can be expanded without restriction. Just some of these subblocks of the start block 12 are therefore shown as an example in Fig. 2. As shown in Fig. 2 the start block 12 includes a so-called crypt block 28, which, roughly speaking, contains information which is relevant to the encryption of the multimedia data. The start block 12 also has a so-called licence block 30, which contains data relating to the way in which a user can or may utilize the encrypted multimedia data stream. The start block 12 also includes a user data info block 32, which can include information relating to the user data block 14 and general information on the start block 12 itself. In addition, the start block 12 may also have an old-start-block block 34, which permits a so-called recursive start block structure. This block enables the user who has not only a decrypting device but also an encrypting device to reformat an encrypted multimedia data stream for other playback devices in his possession without losing or modifying the start block information originally supplied by the distributor. Depending on the application, further subblocks, e.g. an IP information block (IP = Intellectual Property) according to ISO/IEC 14496-1, MPEG-4, Systems, 1998, which contains copyright information, can be included in the start block 12.

As is customary in the field of technology, each block can be designed to have an internal block structure, which first requires a block identifier, then contains the length of the subblock, and then, finally, presents the block user data as such. This increases the flexibility of the encrypted multimedia data stream and in particular that of the start block of the encrypted multimedia data stream in that new demands can be responded to by adding further subblocks and omitting existing subblocks.

Fig. 3 provides an overview of the block user data of the individual subblocks shown in Fig. 2.

The crypt block 28 is considered first. This contains an entry for a multimedia data encryption algorithm 40 which identifies the symmetric encryption algorithm which has been used to encrypt the multimedia data in a preferred embodiment of the present invention. The entry 40 may well be an index for a table such that a decrypting device having read the entry 40 is able to select from among a plurality of encryption algorithms the same encryption algorithm at that used by the encrypting device. The crypt block 28 also includes the entry First step 26, the entry Step 24 and the entry Amount 22, which have already been referred to in connection with Fig. 1. These entries in the start block enable a decrypting device to subdivide an encrypted multimedia data stream appropriately so as to be able to perform decryption correctly.

The crypt block 28 also contains an entry for the distributor or provider or supplier 42 which is a code for the distributor who has generated the encrypted multimedia data stream. An entry User 44 identifies the user who has received the encrypted multimedia data stream in some way or other from the distributor identified by the entry 42. One possible use for these identifiers is to make the user identification device-

specific. The entry User would then contain the serial number of a PC, a laptop, a car hifi device, a home stereo system, etc., which only permits playback on the specific device. To further improve the flexibility and/or security, instead of using the serial number, which has a different structure from one manufacturer to another, but which could be duplicated by chance, a special identification, e.g. a logical coupling of the size of the fixed disk with the processor number etc. in the case of a PC, could be used instead.

An entry 46 contains an output value, which will be discussed in more detail later. This output value represents, generally speaking, an encrypted version of the multimedia data key, which is needed, in conjunction with the multimedia data encryption algorithm identified by the entry 40, in order to correctly decrypt the encrypted multimedia data (sections 16 in Fig. 1) in the user data block 14. To ensure adequate flexibility for future applications, the two entries Output value length 48 and Output value mask 50 have been provided. The entry Output value length 48 indicates the actual length of the output value 46. However, to achieve a flexible start block format more bytes are provided therein for the output value than an output value can actually have at the present time. The output value mask 50 thus indicates how a shorter output value is distributed over a longer output value space. If the output value length is e.g. half as big as the space available for the output value, the output value mask could be so constituted that the first half of the output value mask is set and the second half is not set. The output value would then simply be entered in the space allocated by the syntax for the start block and occupy the first half of this space while the other half is ignored due to the output value mask 50.

The licence block 30 of the start block 12 will now be considered. This includes an entry Bit mask 52. This entry can contain certain special information for playing back or for the general mode of using the encrypted multimedia data. In particular, a decrypting device could be informed in this way whether or not the user data can be played back locally. Furthermore, it could be signalized here whether the challenge-response method described in the German Patent DE 196 25 635 C1 cited earlier and which permits efficient database access has been used for encryption.

An entry Expiration date 54 indicates the date on which permission to decrypt the encrypted multimedia data stream expires. A decrypting device will check the entry Expiration date 54 and compare it with a built-in timer. If the expiration date has been passed, the decrypting device will no longer perform a decryption of the encrypted multimedia data stream. This enables a provider to supply encrypted multimedia data for a limited time period, offering the advantage of a much greater flexibility in the management of the data and in pricing policy. This flexibility is further supported by an entry Start date 56, which specifies when decryption of an encrypted multimedia file may commence. A decrypting device will compare the entry Start date with its own built-in clock and will only start decrypting the encrypted multimedia data when the actual time is later than that specified by the start date 56.

An entry Permitted playbacks 58 specifies how often the encrypted multimedia data stream may be decrypted, i.e. played back. This further increases the flexibility of the provider in that he only permits a certain number of playbacks, e.g. in return for a certain sum which is less than that which would be demanded for the unrestricted use of the encrypted multimedia data stream.

To verify or support the entry Permitted playbacks 58 the licence block 30 has another entry Actual playbacks 60, which could e.g. be incremented by one after each decryption of the encrypted multimedia data stream. A decrypting device will thus always check whether the entry Actual playbacks is less than the entry Permitted playbacks. If this is so, the multimedia data will be decrypted. If not, no further decryption takes place.

The entries Permitted copies 62 and Actual copies 64 are analogues of the entries 58 and 60. By means of the two entries 62 and 64 it is ensured that the user of the multimedia data only copies them as often as he is allowed to do so by the provider or as often as is warranted by the cost of buying the multimedia data. By means of the entries 58 to 64 an effective copyright protection is guaranteed and it is possible to discriminate between private users and commercial users, e.g. by setting the entries Permitted playbacks 58 and Permitted copies 62 to a small value.

Licensing might e.g. be on the basis that a certain number of copies (entry 62) of the original is permitted while no copies of a copy are allowed. The start block of a copy would then, in contrast to the start block of the original, have a zero in the entry Permitted copies, meaning that this copy will not be copied again by a correctly functioning encrypting/decrypting device.

In the example of a multimedia data protection protocol (MMP; MMP = Multimedia Protection Protocol) shown here, the start block 12 also contains a user data information block 32 which has just two block user data entries 66 and 68, the entry 66 containing a hash total over the whole start block and the en-

try 68 identifying the type of hash algorithm which has been used to generate the hash total over the whole start block.

Among the publications which are useful in this connection is the technical book "Applied Cryptography", Second Edition, John Wiley & Sons, Inc. By Bruce Schneier (ISBN 0 471-11709-9) which contains a comprehensive treatment of symmetric encryption algorithms, asymmetric encryption algorithms and hash algorithms.

Finally the start block 12 includes the old-start-block block 34, which in addition to the synchronization information, which is not shown in Fig. 3, contains the entry Old start block 70. If a user performs his own encryption and thus generates a new start block 12, the old start block from the provider can be preserved in the entry Old start block 70 so as not to lose any important information that the provider has written into the start block. This might include copyright information (IP information block), previous user information and distributor information, which make it possible to trace back a multimedia file, which e.g. has been decrypted/encrypted several times by various devices, to the original supplier while preserving copyright information. In this way it is possible to check at all times whether an encrypted multimedia file has been acquired legally or illegally.

It is obvious that the sequence of steps in Fig. 5 can be varied in the same way as explained below with reference to Fig. 4.

Fig. 4 shows a flowchart of the method according to the present invention for generating an encrypted multimedia data stream. In a step 100 the start block 12 is generated. Then, in a step 102, the first part of the multimedia data to be en-

rypted is used as the start section of the user data block 14, but this first part itself is not encrypted. The start section thus forms the further unencrypted section 20 of Fig. 1, whose length is specified in the entry First step 26 in the start block. The second part of the multimedia data to be encrypted is then encrypted in a step 104 to generate the encrypted section 16 which follows the unencrypted section 20 (Fig. 1). To produce a simple encrypted multimedia data stream, the encrypted second part is appended to the start section of the user data block (step 106), so that the encrypted multimedia data stream 10 contains the start block 12, the start section 20 and the encrypted second part 16. The encrypted multimedia data stream can now be extended as desired by generating another unencrypted section 18, an encrypted section 16, etc. and writing them into the user data block 14.

From Fig. 4 it can be seen that there is no fixed sequence for the steps 100 to 106. The start block could also be generated after completion of the user data block and placed at the head of the user data block using a block multiplexer. Alternatively, the second part of the multimedia data to be encrypted could be encrypted (step 104) before the first part is written into the data block since the entry First step 26 defines precisely the point, i.e. the bit position, in the data block 14 at which the encrypted second part must start to be entered. What is important here is simply that the unencrypted start section 20 of the user data block 14 should be placed immediately after the start block 12. It should be emphasized again at this point that the sequence of start block, unencrypted start section and encrypted second part (i.e. 12, 20, 16) described here simply describes the sequence in which the multimedia data stream must be arranged in the playback device so as to exploit the advantages of the present invention. This sequence has no effect on the transmission of the encrypted multimedia data stream. This becomes particularly apparent

when a packet-oriented transmission is used. A packet for the start block, a packet for the start section and a packet for the encrypted second part could be transmitted over different paths from a transmitter to a receiver in such a way that the start section arrives first, followed by the encrypted second part and finally the start block. In this case, of course, the playback device must be capable of rearranging the three packets, as has already been described.

Fig. 5 shows a flowchart of the method according to the present invention for playing back the encrypted multimedia data stream 10 comprising the start block 12, the unencrypted start section 20 of the user data block 14 and the encrypted second part 16 of the user data block 14. According to the present invention only the information of the start block 12 which is absolutely necessary for playing back the unencrypted start section of the user data block 14 (step 110) is initially processed in the playback device.

Subsequently the unencrypted start section 20 of the user data block 14 can be played back with minimal delay (step 112). In this way a simple and efficient preview or prelisten function is achieved. Playing back the start section of the user data block (step 112) will not normally require the full processing power of the playback device. Thus the playback device can, while playing back the start section, also process essentially concurrently the other information of the start block 12, i.e. the information which is not needed to play back the start section of the user data block (step 114). Once the start block 12 has been processed, the playback device will then be able to decrypt the encrypted multimedia data in the first encrypted section 16, i.e. the encrypted second part of the user data block 14 (step 116), thus enabling it to then play back the decrypted multimedia data of the second section (step 118).

The information which is absolutely necessary for playing back the unencrypted start section 20 will now be discussed making reference to Fig. 3. Among the information which is absolutely necessary are the general block identification information and block length information, which are not shown in Fig. 3, which enable a playback device to correctly locate where the necessary information is to be found in the start block. If the multimedia data are coded in some way, as is usually the case, e.g. according to an MPEG method, the playback device will have to extract this information from the start block 12 in step 110 (Fig. 5). In the table in Fig. 3 this information is contained in the entry User data type of the user data block 14. The playback device then knows that the unencrypted data in the start section 20 of the user data block 14 are coded in e.g. MPEG layer 3 format (MP3), so that the playback device can then decode and play back the unencrypted multimedia data (step 112). While the start section 20 is being played back, the device is now able to process all the relatively complicated additional data of the start section, such as the data in the crypt block 28, in the licence block 30 and in the user data information block 32, which in particular contains a relatively complex hash total /digital signature over the start block (entry 66). Another complicated operation is that of decrypting the multimedia data key from the output value (entry 46) so as to be able to decrypt the encrypted sections 16 (Fig. 1) of the encrypted multimedia data stream.

It is possible to specify whether or not the entries Distributor 42 and User 44 should also belong to the necessary information for playing back the unencrypted start section 20. If so, the preview or prelisten function is only available for a particular user or for the subscribers of a particular distributor. This means that, via the very simple and uncomplicated implementation of the preview or prelisten function, a

distributor can send an encrypted multimedia file to a special user or to all his subscription users, who can then listen to or view an extract of e.g. 1 second's to 1 minute's duration, i.e. the unencrypted start section 20. If a user finds this offering to his taste he can then decide to pay for the whole encrypted multimedia data stream. This facility also enables individual items to be identified in a simple manner.

In this case it is not necessary to perform the steps 114, 116 and 118. It should be noted that it is in fact not possible to perform these steps in this case, since the user may not yet possess the information as to how the output value 46 must be decrypted so as to obtain the multimedia data key enabling the encrypted multimedia data in the encrypted sections 16 to be decrypted. Should a user decide to purchase after his appetite has been whetted by the preview or prelisten function, all the distributor has to do is to enable the user to decrypt the output value.

Providing an unencrypted start section in the user data block thus enables the preview or prelisten function to be offered in a simple way and also makes it possible to use processors with limited storage or processing resources without having to put up with significant delays resulting from the processing of the whole start block.

Claims

1. A method for generating an encrypted user data stream [(10)], which has a start block [(12)] and a user data block [(14)], comprising the following steps:

generating [(100)] the start block [(12)]; and

generating [(102, 104, 106)] the user data block [(14)] by means of the following substeps:

using [(102)] a first part of the user data to be encrypted as start section [(20)] for the user data block [(14)], the start section [(20)] being unencrypted;

encrypting [(104)] a second part of user data to be encrypted which follow the first part; and

appending [(106)] the encrypted user data [(16)] to the unencrypted start section [(20)].

2. A method according to claim 1, wherein the step of generating [(100)] the start block [(12)] includes the following substep:

entering the length [(26)] of the start section [(20)] in the start block [(12)].

3. A method according to claim 1 [or 2], wherein the second part does not comprise all the user data to be encrypted and wherein the step of generating [(102, 104, 106)] the user data block includes the following substep:

appending a third part [(18)] of user data to be en-

encrypted, which follow the second part, to the encrypted user data [(16)] of the second part, the user data of the third part being unencrypted.

4. A method according to [one of the preceding claims] claim 1, wherein the step of generating [(100)] the start block [(12)] includes the following substep:

entering the length [(22)] of the encrypted multimedia data [(16)], which correspond to the user data of the second part which are to be encrypted, in the start block [(12)].

5. A method according to claim 3 [or 4], wherein the step of generating [(100)] the start block [(12)] also includes the following substep:

entering the sum [(24)] of the length [(22)] of the encrypted user data, which correspond to the second part, and the length of the third part of the unencrypted user data [(18)] in the start block [(12)].

6. A method for playing back an encrypted multimedia data stream [(10)], which has a start block [(12)] and a user data block [(14)], where a start section [(20)] of the user data block [(14)], which follows the start block [(12)], contains unencrypted user data and where a further section [(16)] of the user data block [(14)] contains encrypted user data, where the start block [(12)] contains information which is needed to play back the start section [(20)] of the user data block [(14)] and where the start block [(12)] contains information which is not needed to play back the unencrypted start section [(20)] of the user data block [(14)], comprising the following steps:

processing [(110)] the information of the start block [(12)] which is needed to play back the start section [(20)] of the user data block [(14)]; and

playing back [(112)] the unencrypted start section [(20)] of the user data block [(14)].

7. A method according to claim 6, which also includes the following steps:

processing [(114)] the information of the start block [(12)] which is not needed to play back the unencrypted start section [(20)];

decrypting the further section [(16)] of the user data block [(14)] using the processed information of the start block [(12)]; and

playing back [(118)] the encrypted user data of the further section [(16)] of the user data block [(14)].

8. A method according to claim 7, wherein the step of processing [(114)] the information of the start block [(12)] which is not needed to play back the unencrypted start section [(20)] is performed essentially concurrently with the playing back [(112)] of the unencrypted start section [(20)].

9. A method according to [one of the claims 6 to 8] claim 6, wherein the length [(22)] of the unencrypted start section [(20)] of the user data block [(14)] is between 1 and 60 seconds.

10. A method according to [one of the claims 6 to 9] claim 6, wherein the user data to be encrypted are coded and wherein the information which is needed for playing back contains an entry [(72)] specifying the type of coding/decoding method.
11. A method according to [one of the preceding claims] claim 1, wherein the user data are audio and/or video data.
12. A device for generating an encrypted user data stream [(10)], which has a start block [(12)] and a user data block [(14)], comprising:
- a unit for generating [(100)] the start block [(12)]; and
- a unit for generating [(102, 104, 106)] the user data block [(14)], with the following features:
- a unit for using [(102)] a first part of the user data to be encrypted as start section [(20)] for the user data block [(14)], the start section [(20)] being unencrypted;
- a unit for encrypting [(104)] a second part of user data to be encrypted which follow the first part; and
- a unit for appending [(106)] the encrypted user data [(16)] to the unencrypted start section [(20)].
13. A device for playing back an encrypted user data stream [(10)], which has a start block [(12)] and a user data block [(14)], where a start section [(20)] of the user data block [(14)], which follows the start block [(12)], contains unencrypted user data and where a further section [(16)] of the user data block [(14)] contains en-

encrypted user data, where the start block [(12)] contains information which is needed to play back the start section [(20)] of the user data block [(14)] and where the start block [(12)] contains information which is not needed to play back the unencrypted start section [(20)] of the user data block [(14)], comprising:

a unit for processing [(110)] the information of the start block [(12)] which is needed to play back the start section [(20)] of the user data block [(14)]; and

a unit for playing back [(112)] the unencrypted start section [(20)] of the user data block [(14)].

14. A device according to claim 13, which further comprises:

a unit for processing [(114)] the information of the start block [(12)] which is not needed to play back the unencrypted start section [(20)];

a unit for decrypting the further section [(16)] of the user data block [(14)] using the processed information of the start block [(12)]; and

a unit for playing back [(118)] the encrypted user data of the further section [(16)] of the user data block [(14)].

15. A device according to claim 14, wherein the unit for processing [(114)] the information of the start block [(12)] which is not needed to play back the unencrypted start section [(20)] is designed to be operated essentially concurrently to the unit for playing back [(112)] the unencrypted start section [(20)].

**Method and Device for Generating an Encrypted User Data Stream
and Method and Device for Playing Back an Encrypted User Data
Stream**

Abstract

In a method for generating an encrypted multimedia data stream a start block [(12)] and then a user data block [(14)] are generated. The start section [(20)] of the user data block contains unencrypted user data and is followed by encrypted user data [(16)]. In this way a preview or prelisten function is implemented in a simple manner. In addition, a playback device can already play back the unencrypted start section [(20)] while the whole start block is being processed so as to obtain a multimedia data key for generating hash totals, etc. This parallel processing makes it possible to use playback devices with limited storage and processing resources without having to accept excessively long delays.

- 1/4 -

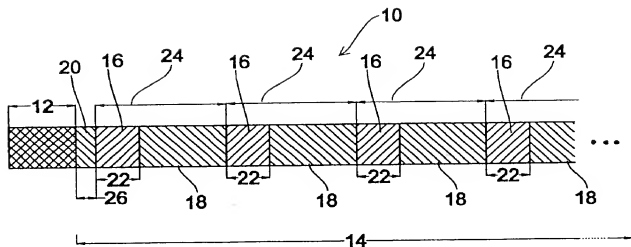


Fig. 1

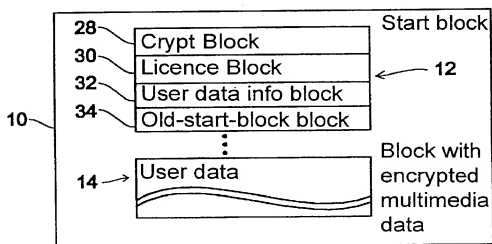


Fig. 2

- 2/4 -

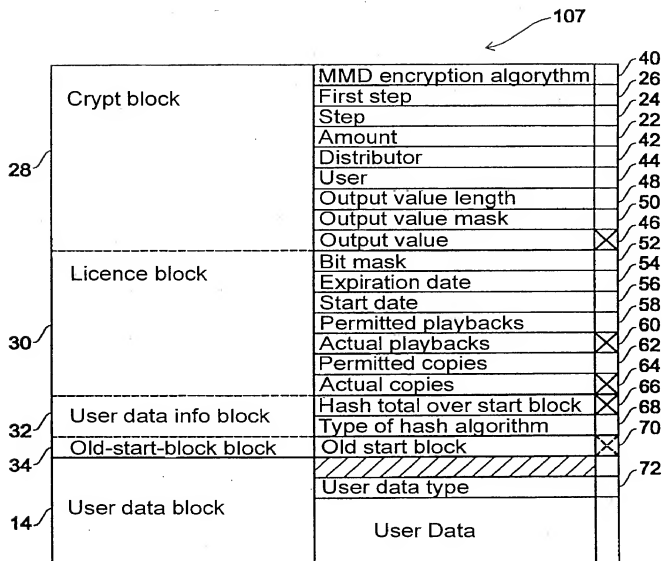


Fig. 3

- 3/4 -

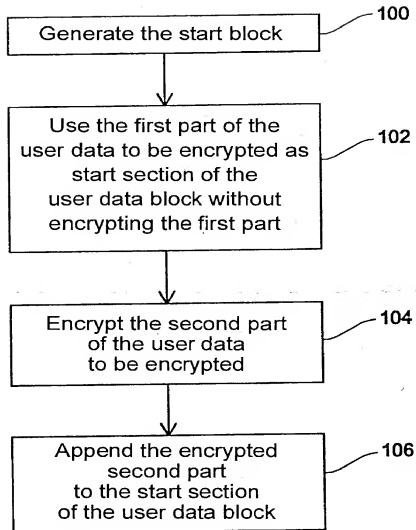


Fig. 4

- 4/4 -

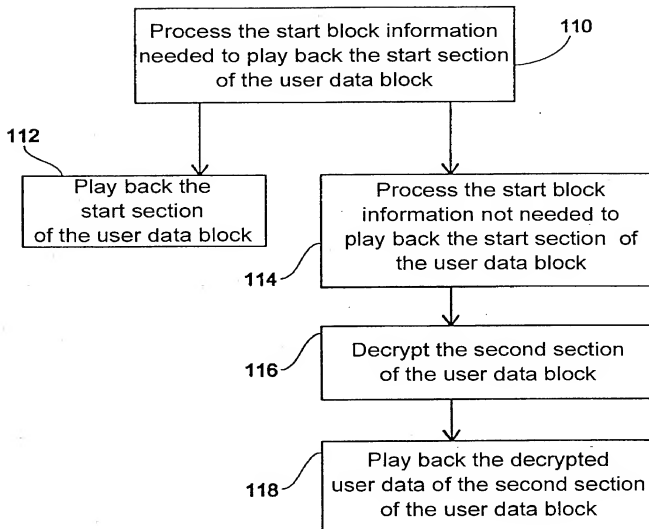


Fig. 5

Practitioner's Docket No. 13189.136

PATENT

COMBINED DECLARATION AND POWER OF ATTORNEY**(ORIGINAL, DESIGN, NATIONAL STAGE OF PCT, SUPPLEMENTAL, DIVISIONAL,
CONTINUATION, OR C-I-P)**

As a below named inventor, I hereby declare that:

TYPE OF DECLARATION

This declaration is for a national stage of PCT application.

INVENTORSHIP IDENTIFICATION

My residence, post office address and citizenship are as stated below, next to my name. I believe that I am an original, first and joint inventor of the subject matter that is claimed, and for which a patent is sought on the invention entitled:

TITLE OF INVENTION

METHOD AND DEVICE FOR GENERATING AN ENCRYPTED USER DATA STREAM AND
METHOD AND DEVICE FOR PLAYING BACK AN ENCRYPTED USER DATA STREAM

SPECIFICATION IDENTIFICATION

The specification was filed on August 16, 2001, as Serial No. 09/913,695.

ACKNOWLEDGMENT OF REVIEW OF PAPERS AND DUTY OF CANDOR

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information, which is material to patentability as defined in 37, Code of Federal Regulations, Section 1.56, and which is material to the examination of this application, namely, information where there is a substantial likelihood that a reasonable Examiner would consider it important in deciding whether to allow the application to issue as a patent.

PRIORITY CLAIM (35 U.S.C. Section 119(a)-(d))

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d) of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed.